

## 

## Confidentiality Notice

*This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage to SURE TRUST or facilitate attacks against SURE TRUST. We shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.*

## Disclaimer

*Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope of the engagement. This report is a summary of the findings from a “point-in-time” assessment made with in SURE TRUST’s environment. Any changes made to the environment during the period of testing may affect the results of the assessment.*

**TABLE OF CONTENTS**

[Confidentiality Notice 1](#_Toc190028120)

[Disclaimer 1](#_Toc190028121)

[**1. EXECUTIVE SUMMARY** 1](#_Toc190028122)

[1.1 Business Risk & Executive Considerations 1](#_Toc190028123)

[1.2 Recommended Actions: 2](#_Toc190028124)

[**2. HIGH LEVEL ASSESSMENT OVERVIEW** 3](#_Toc190028125)

[2.1 Observed Security Strengths 3](#_Toc190028126)

[2.2 Areas for Improvement 3](#_Toc190028127)

[2.2.1 Short Term Recommendations 3](#_Toc190028128)

[2.2.2 Long Term Recommendations 4](#_Toc190028129)

[**3. SCOPE** 5](#_Toc190028130)

[3.1 Networks 5](#_Toc190028131)

[**4.** TESTING METHODOLOGY 7](#_Toc190028132)

[**5.** CLASSIFICATION DEFINITIONS 8](#_Toc190028133)

[5.1 Risk Classifications 8](#_Toc190028134)

[5.2 Exploitation Likelihood Classifications 8](#_Toc190028135)

[5.3 Business Impact Classifications 9](#_Toc190028136)

[5.4 Remediation Difficulty Classifications 9](#_Toc190028137)

[**6.** ASSESSMENT FINDINGS 10](#_Toc190028138)

[**7. CRITICAL VULNERABILITES** 11](#_Toc190028139)

[7.1 SNMP Buffer Overflow 12](#_Toc190028140)

[7.2 Telnet – Unencrypted Communication 14](#_Toc190028141)

[7.3 STARTTLS Command Injection in Dovecot 16](#_Toc190028142)

[7.4 Client-Side Cipher Preference 18](#_Toc190028143)

[**8. HIGH VULNERABILITES** 20](#_Toc190028144)

[8.1 Use of Unsecure Protocol (HTTP) 21](#_Toc190028145)

[8.2 Use of FTP (Unencrypted Protocol) 24](#_Toc190028146)

[8.3 SNMP Remote Information Disclosure in MikroTik Routers 26](#_Toc190028147)

[8.4 SNMP Information Disclosure 28](#_Toc190028148)

[8.5 SWEET32 (CVE-2016-2183) 30](#_Toc190028149)

[**9. MEDIUM VULNERABILITIES** 32](#_Toc190028150)

[9.1 BEAST Attack Vulnerability 33](#_Toc190028151)

[9.2 Anonymous FTP Access (Pure-FTPd) 35](#_Toc190028152)

[9.3 RSA Key Exchange(Weak Forward Secrecy) 37](#_Toc190028153)

[9.4 SSLv2 Offered – Vulnerable to DROWN Attack 39](#_Toc190028154)

[9.5 Logjam Attack Vulnerability 41](#_Toc190028155)

[9.6 BREACH Attack Potential (Gzip HTTP Compression) 43](#_Toc190028156)

[9.7 Prometheus Node Exporter Directory Traversal 45](#_Toc190028157)

[9.8 Weak Cipher Suites 47](#_Toc190028158)

[9.9 RC4 Cipher Vulnerability 48](#_Toc190028159)

[9.10 TLS\_FALLBACK\_SCSV Not Supported 50](#_Toc190028160)

[**10. LOW VULNERABILITES** 52](#_Toc190028161)

[10.1 SSLv3 Offered – Vulnerable to POODLE Attack 53](#_Toc190028162)

[10.2 SSL Sweet32 Attack- Birthday Attack 55](#_Toc190028163)

[10.3 Lucky13 Attack 57](#_Toc190028164)

[**11.** APPENDIX A - TOOLS USED 59](#_Toc190028165)

[**12.** APPENDIX B - ENGAGEMENT INFORMATION 60](#_Toc190028166)

[12.1 Client Information 60](#_Toc190028167)

[12.2 Version Information 60](#_Toc190028168)

[12.3 Contact Information 60](#_Toc190028169)

# **EXECUTIVE SUMMARY**

I, **MUMMADI GOPAL VAMSI KRISHNA** performed a security assessment of the internal corporate network of **SURE TRUST** on 01-01-2025 to 31-01-2025. My penetration test simulated an attack from an external threat actor attempting to gain access to systems within the SURE TRUST corporate network. The purpose of this assessment was to discover and identify vulnerabilities in SURE TRUST’s infrastructure and suggest methods to remediate the vulnerabilities. I identified a total of TWENTY TWO vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **CRITICAL** | **HIGH** | **MEDIUM** | **LOW** |
| **4** | **5** | **10** | **3** |

The highest severity vulnerabilities give potential attackers the opportunity to **gain unauthorized administrative access to critical systems, exfiltrate sensitive data, and execute malicious code, resulting in significant business disruption and reputational damage**. Some of these vulnerabilities could allow attackers to escalate privileges, move laterally across the network, and potentially deploy ransomware or data destruction attacks.In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

## Business Risk & Executive Considerations

While this vulnerability is primarily technical, it presents significant business risks that require executive attention. A successful exploit could lead to **complete device compromise**, allowing attackers to gain unauthorized access, manipulate network traffic, or establish persistent control over affected infrastructure.

Failure to address this issue could result in:

* **Regulatory non-compliance** (e.g., GDPR, HIPAA, or industry-specific security mandates) if sensitive data is exposed.
* **Operational disruptions** due to network outages or malicious modifications.
* **Reputational damage** if attackers exploit the vulnerability for widespread attacks.

## Recommended Actions:

1. **Immediate Patch Deployment** – Ensure that all MikroTik devices are updated with the latest firmware containing security patches.
2. **Network Segmentation** – Restrict SNMP access to trusted sources and disable it if not needed.
3. **Intrusion Detection & Prevention** – Monitor for abnormal SNMP traffic patterns that may indicate exploitation attempts.

# **HIGH LEVEL ASSESSMENT OVERVIEW**

## Observed Security Strengths

I identified the following strengths in SURE TRUST’s network that significantlyimprove the security posture. SURE TRUST should continue to monitor these controls to ensure they remain effective.

Access Controls

* Strong password policies implemented on critical systems.
* Multi-factor authentication (MFA) enabled for remote access.

Network Segmentation

* Segmented network architecture, which limits lateral movement in case of a breach.

Patch Management

* Regular updates and patching were observed on several core systems, reducing the risk of exploitation of known vulnerabilities

## Areas for Improvement

I recommend that SURE TRUST takes the following actions to improve the security of the network. Implementing these recommendations will reduce the likelihood that an attacker will be able to successfully attack SURE TRUST’s information systems and/or reduce the impact of a successful attack.

### Short Term Recommendations

These actions should be taken immediately to minimize business risk:

Vulnerability Management

* Remediate high- and critical-severity vulnerabilities, especially those related to remote code execution (RCE) and privilege escalation.
* Perform regular vulnerability scans and patch management.

Incident Response

* Establish an incident response plan (IRP) and conduct periodic drills to ensure readiness.
* Implement logging and monitoring for all critical systems to detect suspicious activity.

### Long Term Recommendations

The following actions should be taken over the next 6–12 months to address harder-to-remediate issues that pose less immediate risk but are still critical for long-term security.

Security Awareness Training

* Conduct periodic security awareness training for all employees to mitigate phishing and social engineering risks

Network Hardening

* Perform a comprehensive review of firewall rules and access control lists (ACLs) to ensure they follow the principle of least privilege.
* Consider adopting a Zero Trust architecture for long-term security enhancement.

Policy and Compliance Alignment

* Develop and implement security policies and procedures in line with industry standards such as **ISO 27001** or **NIST Cybersecurity Framework**. Regularly review and update these policies to ensure compliance with evolving security regulations.

# **SCOPE**

All testing was based on the scope as defined in the Request For Proposal (RFP) and official written communications. The items in scope are listed below.

## Networks

|  |  |
| --- | --- |
| **Network** | **Note** |
| 47.241.101.3 | Alibaba Cloud - SG |
| 67.20.124.65 | Unified Layer |
| 191.82.121.191 | Telefonica de Argentina |
| 124.117.225.66 | From Xinjiang Network of ChinaTelecom |
| 185.146.86.135 | ORG-CWS5-RIPE |
| 194.110.254.16 | ORG-TL914-RIPE |
| 103.23.227.37 | Universitas Sebelas Maret |
| 20.239.145.15 | Microsoft Corporation (MSFT) |
| 102.212.121.116 | ORG-NWIS1-AFRINIC |
| 184.164.141.29 | SECURED SERVERS LLC (SSL-65) |
| 106.225.244.11 | CHINANET JIANGXI PROVINCE NETWORK |
| 103.56.148.203 | PT Beon Intermedia |
| 47.108.37.191 | Aliyun Computing Co., LTD |
| 34.54.120.230 | Google LLC (GOOGL-2) |
| 185.216.120.11 | de-buerodata-broadband |
| 187.251.108.186 | TOTAL PLAY TELECOMUNICACIONES SA DE CV |
| 144.217.240.87 | OVH Hosting, Inc. (HO-2) |
| 51.79.65.16 | OVH Hosting, Inc. (HO-2) |
| 198.245.53.101 | OVH Hosting, Inc. |
| 149.56.129.34 | OVH Hosting, Inc |
| 184.74.137.227 | Charter Communications Inc (CC-3517) |
| 95.86.76.47 | Internet Rimon |
| 207.148.103.159 | TYO\_VULTR\_CUST |
| 2.74.193.188 | "KCell" JSC |
| 105.235.122.97 | AfriNIC Whois serve |
| 142.132.207.118 | ORG-HOA1-RIPE |
| 219.94.189.215 | SAKURA Internet Inc. |
| 88.198.137.134 | ORG-HOA1-RIPE |
| 5.135.137.222 | OVH SAS Dedicated servers |
| 128.32.220.18 | University of California at Berkeley (UCAB-1-Z) |
| 2.152.66.8 | ONO\_HFC |

# TESTING METHODOLOGY

My testing methodology was split into three phases: **Reconnaissance**, **Target Assessment**, and **Execution of Vulnerabilities**. During reconnaissance, I gathered information about SURE TRUST’s network systems. I used port scanning, service enumeration, and OS fingerprinting to refine target information and assess potential vulnerabilities.

Next, I conducted the **Targeted Assessment**, simulating an attacker exploiting vulnerabilities in the SURE TRUST network. During this phase, I identified and tested vulnerabilities while ensuring minimal disruption to normal business operations.

Evidence of vulnerabilities was gathered throughout the engagement to provide detailed findings and recommendations for remediation.

The following image is a graphical representation of this methodology.

# CLASSIFICATION DEFINITIONS

## Risk Classifications

|  |  |  |
| --- | --- | --- |
| **Level** | **Score** | **Description** |
| **Critical** | **10** | Immediate threat to the organization. Successful exploitation can cause severe, permanent damage. Immediate remediation is required. |
| **High** | **7-9** | Urgent threat. Exploitation can cause significant business disruption. Prioritize remediation. |
| **Medium** | **4-6** | Exploitation is possible, potentially disrupting business operations. Remediate when feasible. |
| **Low** | **1-3** | Minimal threat with low impact. Remediation is recommended but not urgent. |
| **Informational** | **0** | No direct threat but may expose sensitive information or cause business processes to behave differently. |

## Exploitation Likelihood Classifications

|  |  |
| --- | --- |
| **Likelihood** | **Description** |
| **Likely** | Exploitation methods are well-known and can be executed using publicly available tools with minimal effort. Low-skilled attackers can exploit this vulnerability. |
| **Possible** | Exploitation requires public tools and some configuration knowledge. Understanding of the underlying system is needed. |
| **Unlikely** | Exploitation requires advanced technical skills and specific conditions, making it difficult to achieve. |

## Business Impact Classifications

|  |  |
| --- | --- |
| **Impact** | **Description** |
| **Major** | Large-scale disruptions to critical business functions. Significant financial loss. |
| **Moderate** | Disruption of non-critical business functions with some impact. |
| **Minor** | Minimal impact on few users with no major disruption. |

## Remediation Difficulty Classifications

|  |  |
| --- | --- |
| **Difficulty** | **Description** |
| **Hard** | Requires extensive reconfiguration, may disrupt business operations, and is time-consuming.. |
| **Moderate** | Involves minor reconfigurations or additions that may take time or incur costs. |
| **Easy** | Can be remediated quickly with minimal effort. |

# ASSESSMENT FINDINGS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Number** | **Finding** | **Risk Score** | **Risk** | **Page** |
| 1 | SNMP Buffer Overflow | **9.8** | **Critical** | 12 |
| 2 | Telnet – Unencrypted Communication | **9.1** | **Critical** | 14 |
| 3 | STARTTLS Command Injection in Dovecot | **9.1** | **Critical** | 16 |
| 4 | Client-Side Cipher Preference | **9.1** | **Critical** | 18 |
| 5 | Use of Unsecure Protocol (HTTP) | **8.2** | **High** | 21 |
| 6 | Use of FTP (Unencrypted Protocol) | **8.2** | **High** | 24 |
| 7 | SNMP Remote Information Disclosure in MikroTik Routers | **7.5** | **High** | 26 |
| 8 | SNMP Information Disclosure | **7.5** | **High** | 28 |
| 9 | SWEET32 (CVE-2016-2183) | **7.5** | **High** | 30 |
| 10 | BEAST (Browser Exploit Against SSL/TLS) Vulnerability | **6.8** | **Medium** | 33 |
| 11 | Anonymous FTP Access (Pure-FTPd) | **6.5** | **Medium** | 35 |
| 12 | RSA Key Exchange(Weak Forward Secrecy) | **6.5** | **Medium** | 37 |
| 13 | SSLv2 Offered – Vulnerable to DROWN Attack | **5.9** | **Medium** | 39 |
| 14 | Logjam Attack Vulnerability | **5.9** | **Medium** | 41 |
| 15 | BREACH Attack Potential (Gzip HTTP Compression) | **5.9** | **Medium** | 43 |
| 16 | Prometheus Node Exporter Directory Traversal | **5.3** | **Medium** | 45 |
| 17 | Weak Cipher Suites | **5.3** | **Medium** | 47 |
| 18 | RC4 Cipher Vulnerability | **4.3** | **Medium** | 48 |
| 19 | TLS\_FALLBACK\_SCSV Not Supported | **4.3** | **Medium** | 50 |
| 20 | SSLv3 Offered – Vulnerable to POODLE Attack | **3.7** | **Low** | 53 |
| 21 | Sweet32 Attack – Birthday Attack Against 64-bit Block Ciphers in TLS & SSH | **3.1** | **Low** | 55 |
| 22 | Lucky13 Attack | **2.1** | **Low** | 57 |

TEMPLATE NOTE: (Sorting by descending risk score)

# **CRITICAL VULNERABILITES**

CRITICAL VULNERABILITIES

## SNMP Buffer Overflow

**CVSS Score:** 9.8

[Cite your source here.]

**Description:**

**CVE-ID**: CVE-2022-43716

[Cite your source here.]

A **buffer overflow vulnerability** in MikroTik’s SNMP implementation can lead to **remote code execution**. Attackers can send specially crafted SNMP packets to overflow the buffer, allowing them to execute arbitrary code and compromise the device completely.



**Affected IP:** 102.212.121.116

**Affected Port:** UDP/161

**Technical Impact:**

**Remote Code Execution (RCE)**: Attackers can gain control over the router.

**Full System Compromise**: Allows installation of malware or control over the network infrastructure.

**Mitigation:**

**Disable SNMP v1** entirely.

**Enforce SNMPv3** with authentication and encryption.

**Upgrade RouterOS** to the latest stable release with security patches.

Restrict SNMP access to trusted IP addresses via firewall rules.

**Reference:**

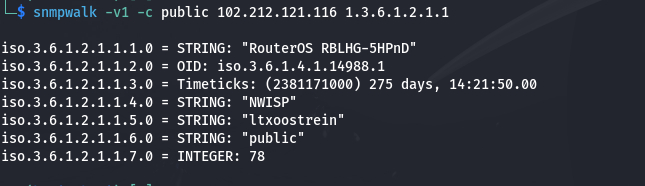
[CVE-2022-43716 on NVD](https://nvd.nist.gov/vuln/detail/CVE-2022-43716)

[MikroTik SNMP Configuration Guide](https://help.mikrotik.com/docs/spaces/ROS/pages/8978519/SNMP)

[OWASP SNMP Security Guide](https://chatgpt.com/g/g-j4PQ2hyqn-ethical-hacker-gpt/c/67a784dc-329c-8005-b82e-92b091ba3343#:~:text=OWASP%20SNMP%20Security%20Guide)

**Proof Of Concept:**

|  |
| --- |
| snmpwalk -v1 -c public <target-ip> 1.3.6.1.2.1.1 |



## Telnet – Unencrypted Communication

**CVSS Score:** 9.1

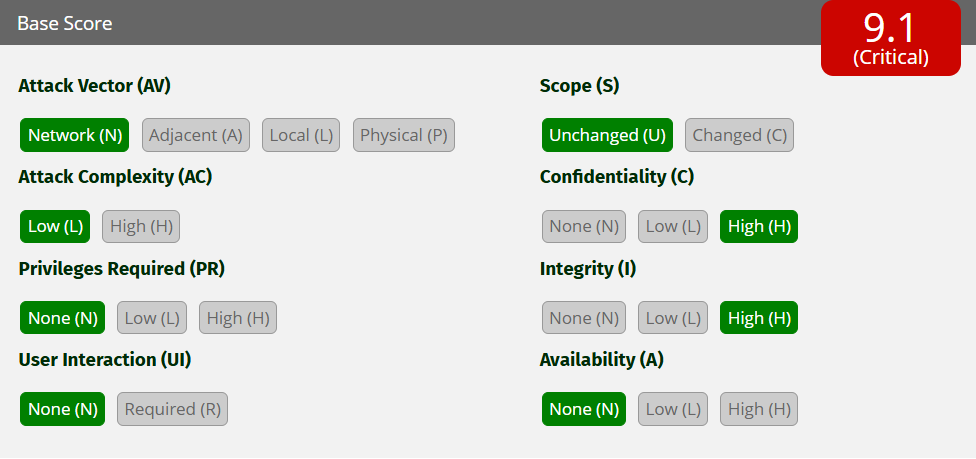
[Cite your source here.]

**Description:**

**CVE-ID**: N/A

[Cite your source here.]

Telnet transmits data in plaintext, including login credentials, making it highly vulnerable to interception and man-in-the-middle (MitM) attacks.



**Affected IP:** 124.117.225.66

191.82.121.191

184.74.137.227

2.74.193.188

105.235.122.97

142.132.207.118

95.86.76.47

2.74.193.188

105.235.122.97

142.132.207.118

**Affected Ports:** TCP/2323, TCP/23

**Technical Impact:**

Credential theft and unauthorized access.

**Mitigation:**

Disable Telnet and use SSH for remote management.

If necessary, restrict Telnet access and use encrypted tunnels.

**Reference:**

[Telnet and Unencrypted FTP Warnings](https://community.tenable.com/s/question/0D53a00008ukBj8CAE/telnet-and-unencrypted-ftp-warnings?language=en_US)

[Preventing Telnet access](https://www.ibm.com/docs/en/i/7.5?topic=security-preventing-telnet-access)

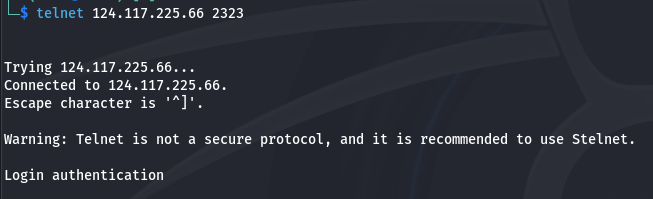
**Proof Of Concept:**

Scanning for the service if it is open

|  |
| --- |
| Nmap -p 23,2323 <target ip> |



|  |
| --- |
| telnet <target ip> <telnet port> |



## STARTTLS Command Injection in Dovecot

**CVSS Score:** 9.1

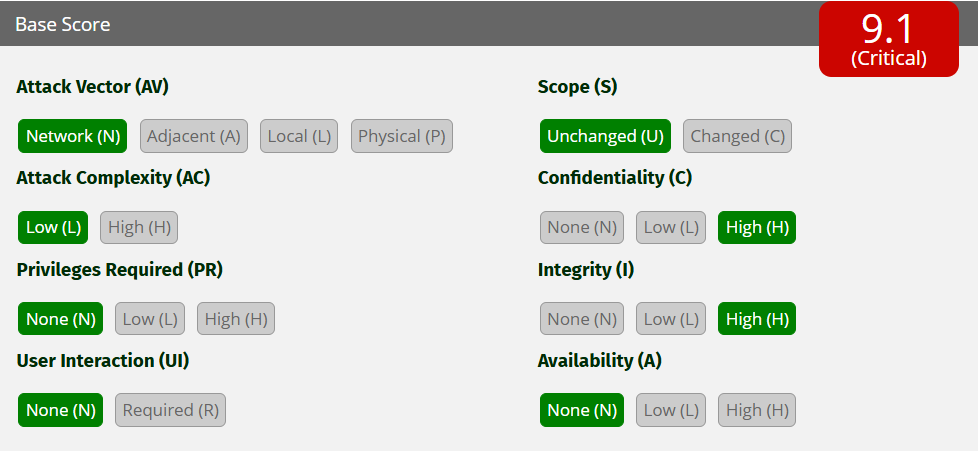
[Cite your source here.]

**Description:**

**CVE-ID**: CVE-2021-33515

[Cite your source here.]

In Dovecot before version **2.3.15**, the **submission service** is vulnerable to a **STARTTLS command injection** in lib-smtp. An attacker can inject commands during the STARTTLS negotiation process, potentially redirecting **sensitive information** (e.g., login credentials or email data) to an attacker-controlled address. This vulnerability can facilitate **man-in-the-middle (MitM)** attacks or **data theft**.



**Affected IP:** 185.146.86.135

**Affected Port:** TCP/143

**Technical Impact:**

**Sensitive Data Exposure**: Credentials or email data may be captured by an attacker.

**Man-in-the-Middle (MitM) Attacks**: Attackers can impersonate the server to intercept private communication.

**Data Breach**: Compromises the confidentiality and integrity of email transmissions

**Mitigation:**

**Upgrade to Dovecot version 2.3.15** or later.

**Disable STARTTLS** where feasible, or enforce strict TLS policies.

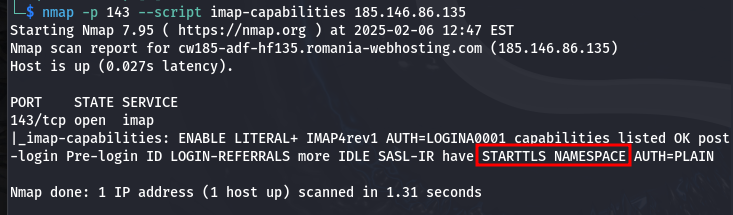
Monitor and log SMTP connection patterns for unusual activity.

**Reference:**

[NIST CVE-2021-33515](https://nvd.nist.gov/vuln/detail/CVE-2021-33515)

[Dovecot Official Documentation](https://www.dovecot.org/)

**Proof Of Concept:** here



## Client-Side Cipher Preference

**CVSS Score:** 9.1

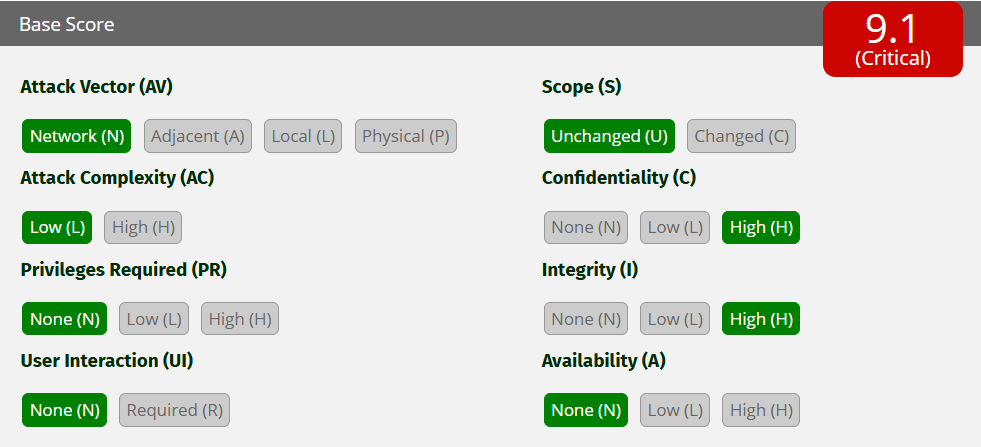
[Cite your source here.]

**Description:**

**CVE-ID**: CVE-2015-2319

[Cite your source here.]

When the server allows the **client to dictate the cipher preference**, it becomes vulnerable to **downgrade attacks**. An attacker could force the client to select a **weaker cipher** (such as one with known vulnerabilities), reducing the security of the connection. This could expose encrypted communication to interception and decryption.



**Affected IP:** 185.146.86.135

**Affected Port:** TCP/143

**Technical Impact:**

**Man-in-the-Middle (MitM) Attack**

**Decryption of Encrypted Data**

**Session Hijacking**

**Mitigation:**

**Enforce Server-Side Cipher Preference** to ensure only secure, recommended ciphers are used.

**Disable deprecated protocols and weak ciphers**, such as TLS 1.0, 1.1, and CBC mode ciphers.

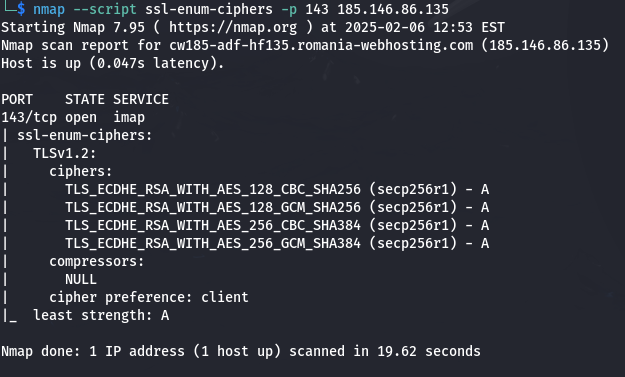
**Enable TLS 1.3** wherever possible for modern cipher security.

**Reference:**

[Cipher preferences and TLS server profiles](https://www.ibm.com/docs/en/datapower-gateway/10.6.0?topic=profile-cipher-preferences-tls-server-profiles)

**Proof Of Concept: \**

here



# **HIGH VULNERABILITES**

HIGH   
 VULNERABILITIES

## Use of Unsecure Protocol (HTTP)

**CVSS Score:** 8.2

[Cite your source here.]

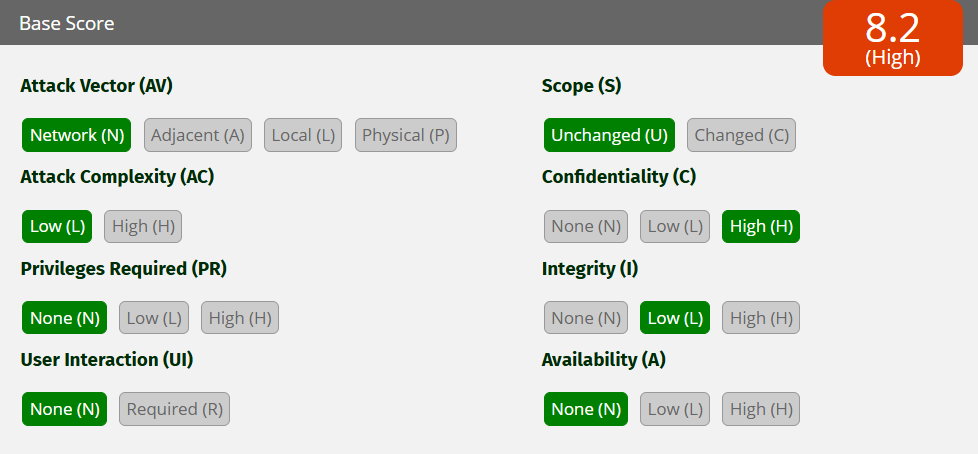
**Description**

**CVE-ID**: N/A

[Cite your source here.]

Any service that communicates over **HTTP instead of HTTPS** is inherently vulnerable to **Man-in-the-Middle (MitM) attacks**, **data interception**, and **manipulation**. This is a significant security risk for **Prometheus Node Exporter** or any other web-based service, exposing sensitive information such as **system metrics, user credentials, session tokens, or configuration details** to unauthorized parties.

Attackers can easily intercept this traffic on an open network and exploit it for reconnaissance or subsequent attacks.



**Affected IP:**

67.20.124.65

191.82.121.191

185.146.86.135

102.212.121.116

184.164.141.29

106.225.244.11

103.56.148.203

47.108.37.191

185.216.120.11

184.74.137.227:1111

95.86.76.47

2.74.193.188

142.132.207.118

219.94.189.215

5.135.137.222

128.32.220.18

47.241.101.3:8083

102.212.121.116:90

184.164.141.29:9100

185.216.120.11:5100

144.217.240.87:9100

144.217.240.87:4444

149.56.129.34:8081

184.74.137.227:1111

**Affected Port:** TCP/80

**Technical Impact:**

* **Information Disclosure**: Metrics data or application-level details can be intercepted in plaintext.
* **Data Manipulation**: An attacker could modify the data in transit, leading to inaccurate monitoring or false alerts.
* **Session Hijacking**: If session tokens or cookies are exposed, attackers can hijack the user session.
* **Increased Risk of Advanced Attacks**: Sensitive data may aid in subsequent privilege escalation or lateral movement within the network.

**Mitigation:**

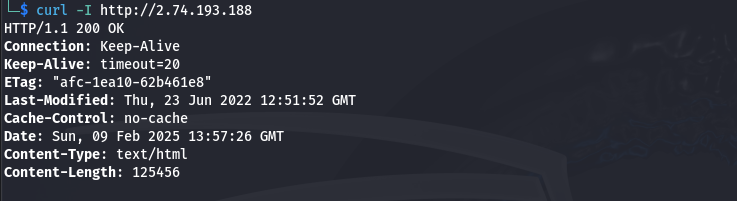
1. **Enforce HTTPS**:
   * Install and configure **TLS certificates** for all services.
   * Use **Let's Encrypt** or other certificate authorities to obtain certificates.
2. **Implement Reverse Proxies**: Configure **NGINX** or **Traefik** to provide HTTPS support for services that do not natively support TLS.
3. **Restrict Access**: Limit public access to services using **firewalls** and allow access only from trusted IPs.
4. **Monitor for HTTP Usage**: Use automated tools to scan for exposed services using HTTP on open ports.

**Reference:** https://

**Proof Of Concept:** here

**1. Test for HTTP Exposure:**  
Use curl to check whether the service is using HTTP:

curl -I http://<target-ip>



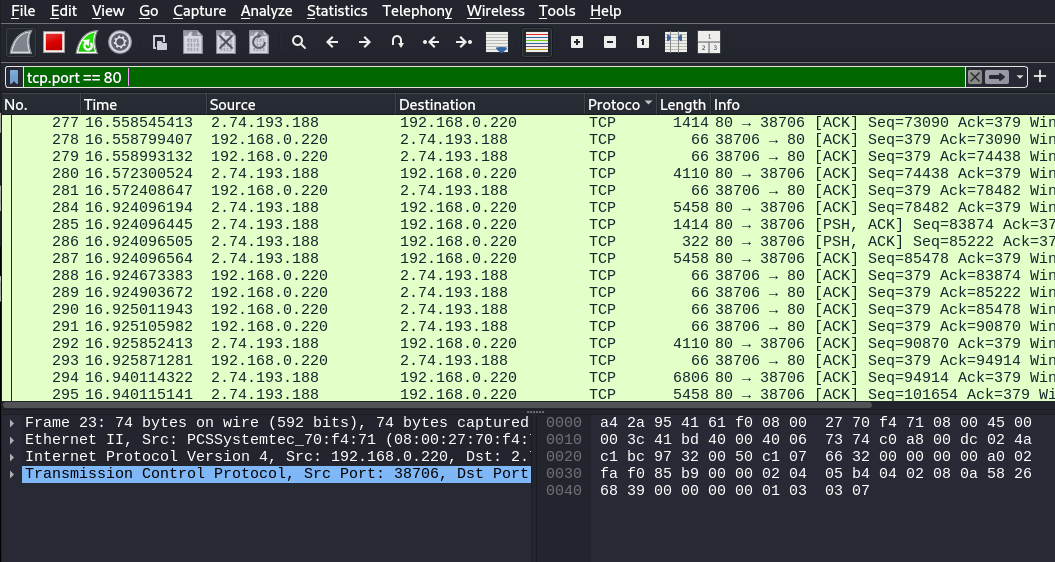
**Example Response:**

HTTP/1.1 200 OK

Content-Type: text/html; charset=UTF-8

**2. Intercept HTTP Traffic with Wireshark:**

* Start capturing network traffic with Wireshark.
* Filter traffic using the expression:



tcp.port == 80

* Analyze captured packets and observe that the transmitted data is in plaintext.

## Use of FTP (Unencrypted Protocol)

**CVSS Score:** 8.2

[Cite your source here.]

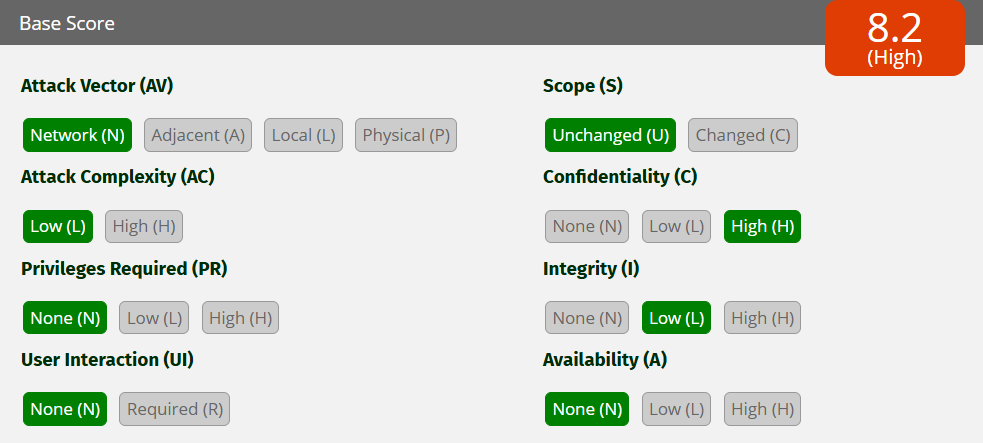
**Description:**

**CVE-ID**: N/A

[Cite your source here.]

**FTP (File Transfer Protocol)** is an outdated and insecure protocol that transmits data, including **usernames and passwords**, in **plaintext**. Since it does not support encryption, attackers can intercept the traffic and steal sensitive information using **Man-in-the-Middle (MitM) attacks**.

FTP is vulnerable to **brute-force attacks**, **session hijacking**, and **data manipulation**. The lack of encryption makes it particularly dangerous on untrusted networks, such as public or shared environments.



**Affected IP:**

67.20.124.65

185.146.86.135

20.239.145.15

102.212.121.116

103.56.148.203

34.54.120.230

185.216.120.11

184.74.137.227

95.86.76.47

219.94.189.215

5.135.137.222

**Affected Port:** TCP/23

**Technical Impact:**

**Credential Theft**: Usernames and passwords can be intercepted in plaintext.

**Data Manipulation**: Attackers can modify files during transfer without detection.

**Information Disclosure**: Files and commands sent over the network can be easily read.

**Brute-Force Attacks**: FTP servers often lack built-in protection mechanisms, making them prone to brute-force login attempts.

**Mitigation:**

**Disable FTP** and use secure alternatives:

* **SFTP (SSH File Transfer Protocol)**
* **FTPS (FTP over TLS/SSL)**

**Restrict Access**: Apply firewall rules to allow FTP connections only from trusted IP addresses.

**Enable Strong Authentication**: Use key-based authentication for SFTP to prevent password attacks.

**Monitor Logs**: Regularly review server logs for suspicious activities.

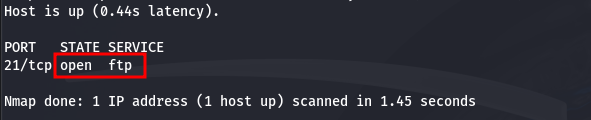
**Reference:**

[OWASP Insecure Protocols Guide](https://owasp.org/www-community/How_to_write_insecure_code)

[NIST Guide to Secure File Transfer](https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-45ver2.pdf)

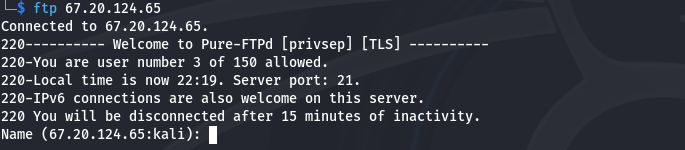
**Proof Of Concept:**

Scan the port



**Test FTP Connection with Command Line:**

|  |
| --- |
| ftp <target-ip> |



## SNMP Remote Information Disclosure in MikroTik Routers

**CVSS Score:** 7.5

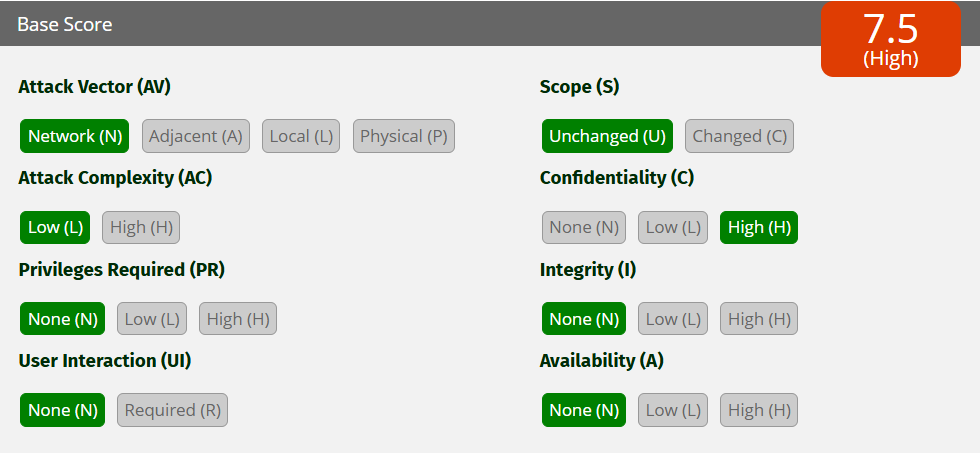
[Cite your source here.]

**CVE-ID**: CVE-2019-3943

[Cite your source here.]

**Description:**

In older versions of MikroTik routers, **SNMP v1** is vulnerable to **remote information disclosure**. This version of SNMP does not implement authentication or encryption, allowing unauthenticated attackers to extract sensitive system information, such as **device uptime, configuration details, and the system description**, through simple queries. This can help attackers in reconnaissance and planning further attacks.



**Affected IP:** 103.23.227.37

**Affected Port:** UDP/161

**Technical Impact:**

**Information Disclosure**: Attackers can gather information about the router’s system, network configuration, and services running.

**Reconnaissance and Attack Planning**: Collected details can be used to exploit other vulnerabilities or identify network topology.

**Mitigation:**

**Disable SNMP v1 and v2c** on MikroTik devices.

**Enable SNMPv3**, which supports authentication and encryption.

**Apply firewall rules** to restrict SNMP access to trusted IP addresses.

**Upgrade MikroTik RouterOS** to the latest stable version with security patches.

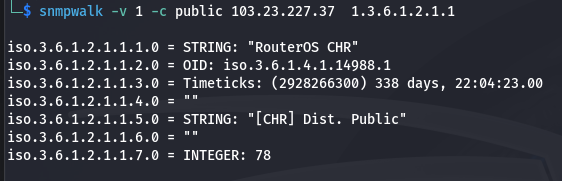
**Reference:**

[NVD CVE-2019-3943](https://nvd.nist.gov/vuln/detail/CVE-2019-3943)

[MikroTik SNMP Documentation](https://help.mikrotik.com/docs/spaces/ROS/pages/8978519/SNMP)

**Proof Of Concept:**

|  |
| --- |
| snmpwalk -v 1 -c public <target> 1.3.6.1.2.1.1 |



## SNMP Information Disclosure

**CVSS Score:** 7.5

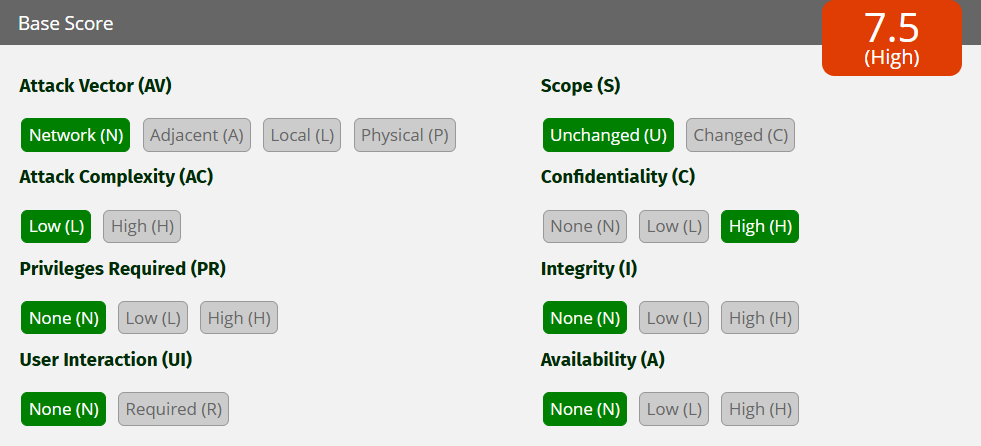
[Cite your source here.]

**Description:**

**CVE-ID**: CVE-2019-3943

[Cite your source here.]

**SNMP v1** allows **unauthenticated access** to sensitive system information such as **router uptime, configuration details, and network settings**. This makes it easy for attackers to gather data for further attacks, including identifying other vulnerabilities.



**Affected IP:** 103.23.227.37

**Affected Port:** UDP/161

**Technical Impact:**

**Reconnaissance**: Attackers can use the leaked information for network mapping and planning attacks.

**Information Disclosure**: Exposes sensitive data that could compromise network security

**Mitigation:**

**Disable SNMP v1 and v2c**; use **SNMPv3** exclusively.

Apply **access control lists (ACLs)** to limit SNMP access to trusted hosts.

Regularly monitor SNMP logs for suspicious activities.

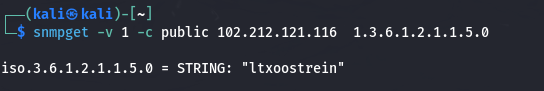
**Reference:**

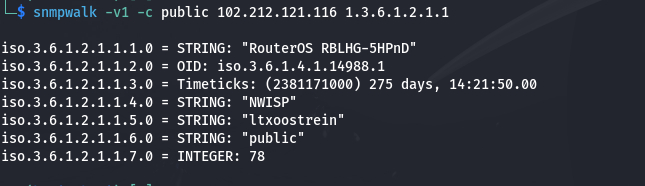
[CVE-2019-3943 on NVD](https://nvd.nist.gov/vuln/detail/CVE-2019-3943)

**Proof Of Concept:**

Use **snmpwalk** to retrieve sensitive data

|  |
| --- |
| snmpwalk -v1 -c public <target-ip> 1.3.6.1.2.1.1 |





## SWEET32 (CVE-2016-2183)

**CVSS Score:** 7.5

[Cite your source here.]

**Description:**

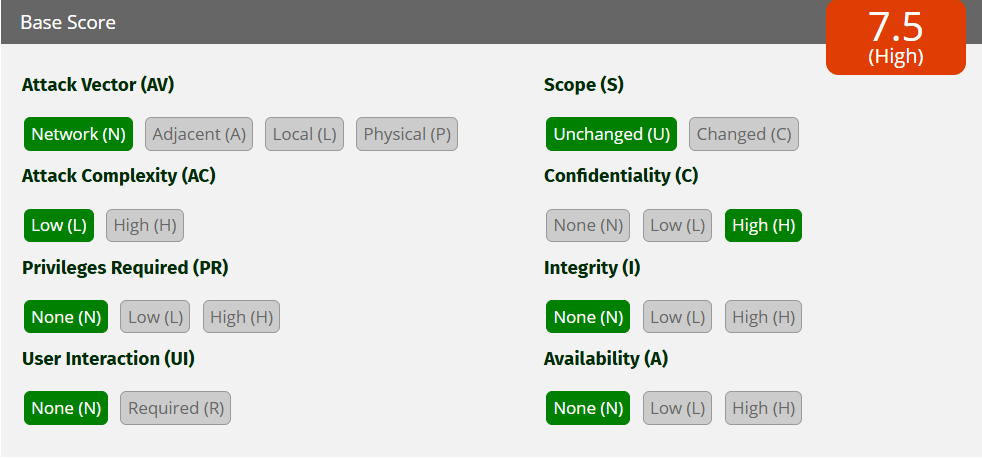
**CVE-ID**: CVE-2016-2183

[Cite your source here.]

The presence of **3DES (DES-CBC3-SHA)** makes the server vulnerable to **SWEET32**.

SWEET32 exploits **birthday attacks** on block ciphers with a 64-bit block size

**CVSS Metrics:**



**Affected IP:** 47.241.101.3

**Affected Port:** TCP/50001

**Technical Impact:**

Attackers can decrypt traffic if they capture a large amount of encrypted data.

Affects VPNs and web servers using outdated cipher suites.

**Mitigation:**

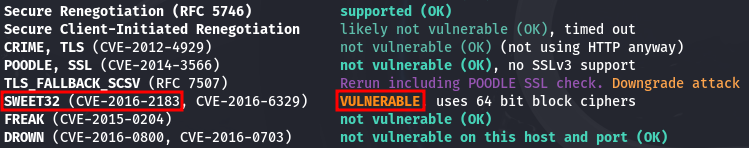
Disable **3DES (DES-CBC3-SHA)** and use AES-GCM instead

**Reference:**

[SWEET32 Advisory](https://sweet32.info/)

**Proof Of Concept:**

To check if 3DES is supported:



# **MEDIUM VULNERABILITIES**

medium VULNERABILITIES

## BEAST Attack Vulnerability

**CVSS Score:** 6.8

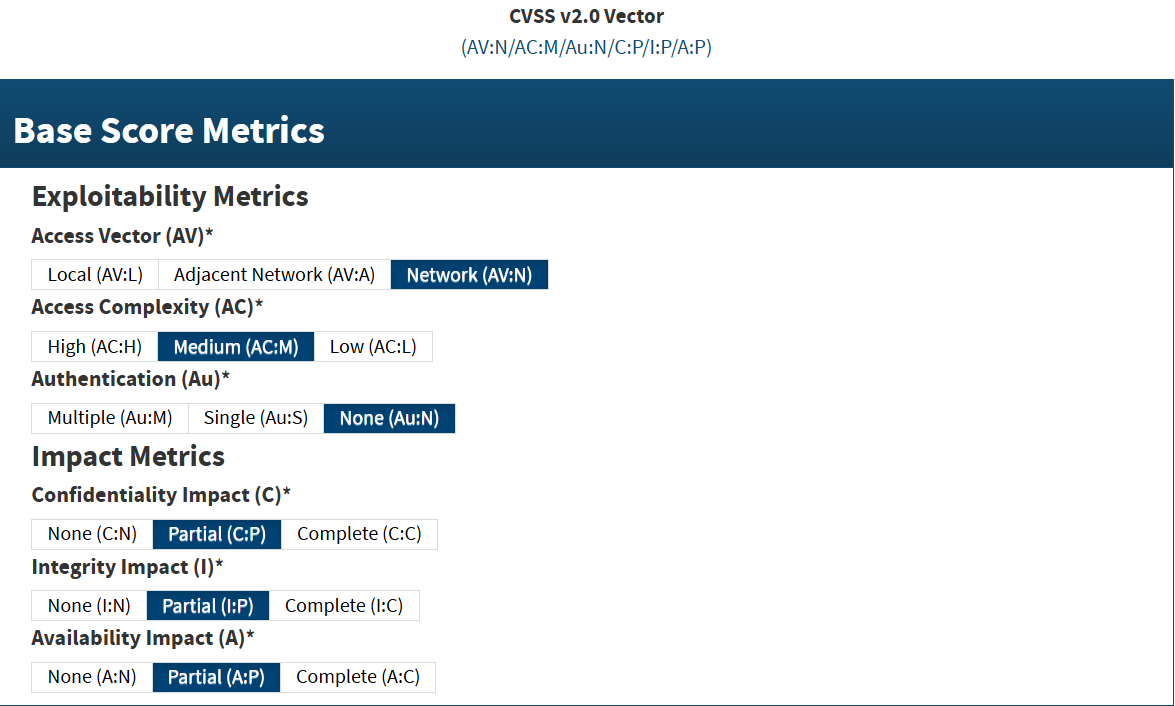
[Cite your source here.]

**Description:**

**CVE-ID**: CVE-2011-3389

[Cite your source here.]

TLS 1.0 is vulnerable to the **BEAST** attack, which exploits weaknesses in **CBC-mode ciphers**.



**Affected IP:** 47.241.101.3

103.56.148.203

47.108.37.191

20.239.145.15

**Affected Port:** TCP/50001, TCP/443

**Technical Impact:**

An attacker can decrypt session cookies and other sensitive data.

**Mitigation:**

Disable **TLS 1.0** and **CBC-mode ciphers**.

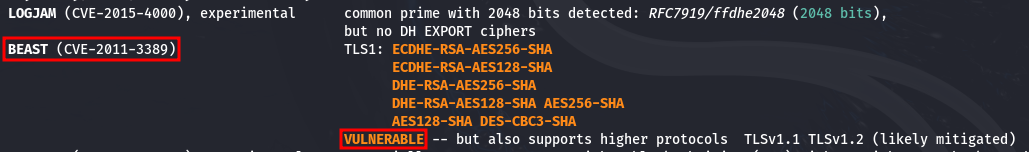
Prioritize AES-GCM and TLS 1.2+.

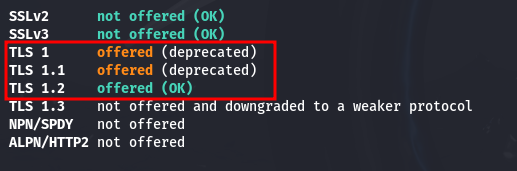
**Reference:**

BEAST Attack

**Proof Of Concept:**

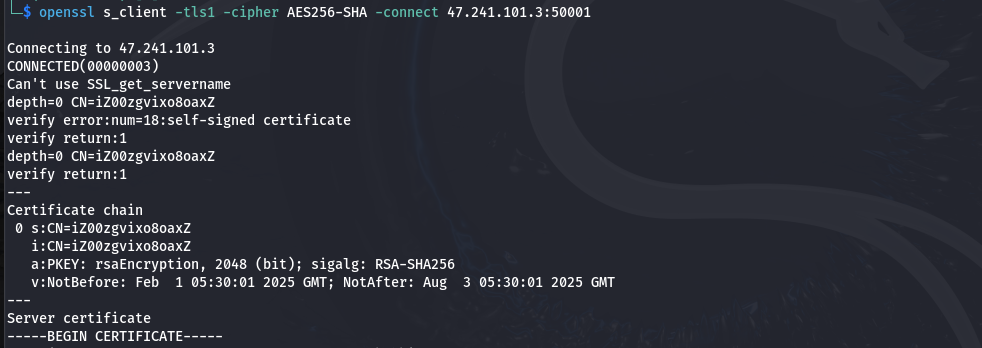
here





Check for **BEAST** vulnerability:

|  |
| --- |
| openssl s\_client -tls1 -cipher AES256-SHA -connect 47.241.101.3:50001 |



## Anonymous FTP Access (Pure-FTPd)

**CVSS Score:** 6.5

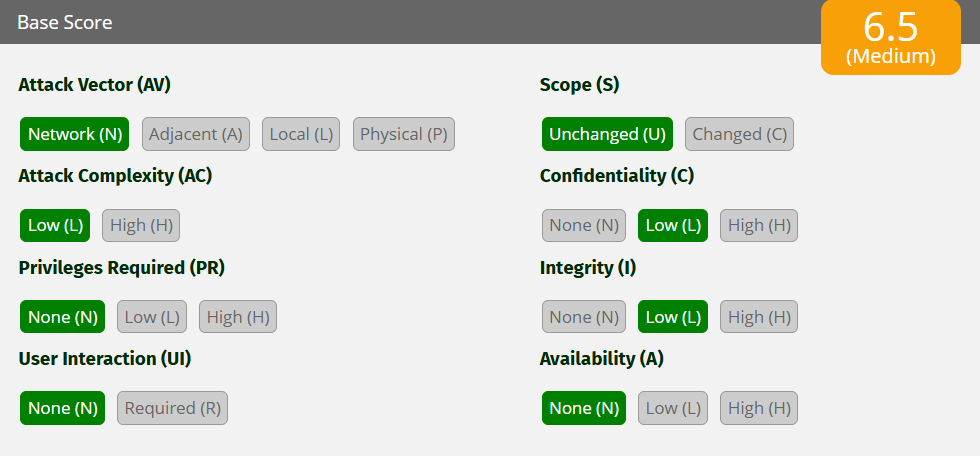
[Cite your source here.]

**Description:**

**CVE-ID**: N/A

[Cite your source here.]

Pure-FTPd allows anonymous login, which can lead to unauthorized access to sensitive files and server resources.



**Affected IP:** 67.20.124.65

**Affected Port:** TCP/21

**Technical Impact:**

Data leakage and unauthorized access to server directories.

**Mitigation:**

Disable anonymous login (NO\_ANONYMOUS=yes in Pure-FTPd configuration).

Enforce strong authentication and use TLS encryption for FTP connections.

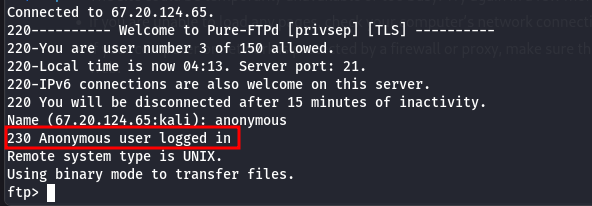
**Reference:**

[Pure-FTPd Documentation](https://www.pureftpd.org/project/pure-ftpd/doc/)

**Proof Of Concept:**

Here is the Commands to connect to the file transfer protocol

|  |
| --- |
| ftp 67.20.124.65  Name: anonymous Password: (leave blank) |



Successful login confirms vulnerability

## RSA Key Exchange(Weak Forward Secrecy)

**CVSS Score:** 9.0

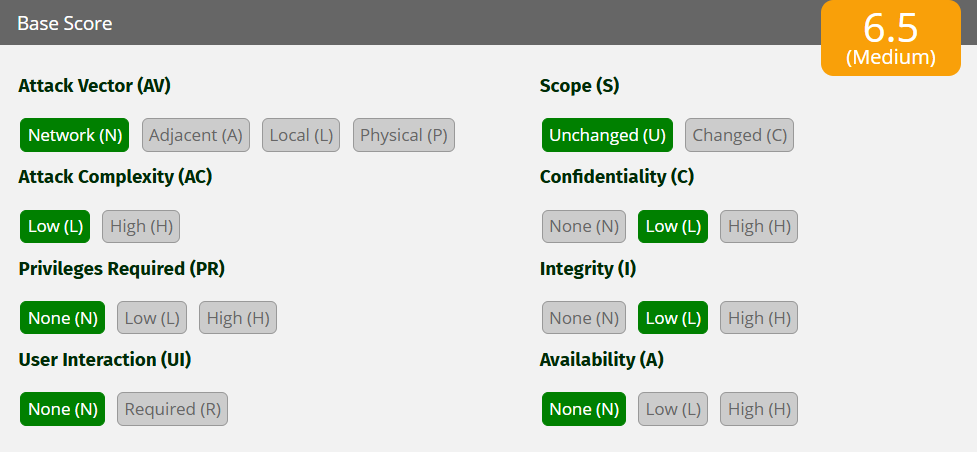
[Cite your source here.]

**Description:**

**CVE-ID**: N/A

[Cite your source here.]

Ciphers that use **RSA for key exchange** (such as TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA) **do not provide Perfect Forward Secrecy (PFS)**. This means that if the private key is compromised, all previous communications can be decrypted retroactively.



**Affected IP:** 185.146.86.135

**Affected Port:** TCP/443

**Affected Ciphers:** RSA

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA

**Technical Impact:**

**Loss of Confidentiality**: Past encrypted communications can be decrypted.

**Increased Risk if Private Key is Leaked**

**Mitigation:**

**Disable RSA-based key exchange ciphers**.

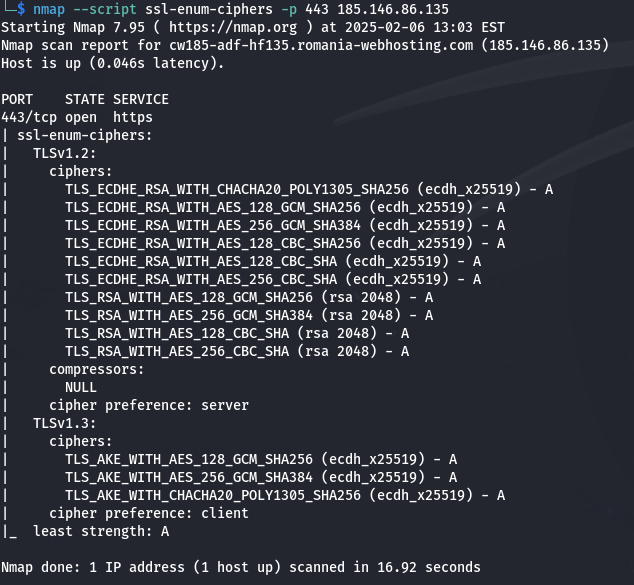
Use only **Elliptic Curve Diffie-Hellman (ECDHE)** ciphers to ensure PFS.

Configure the server to prioritize modern ciphers with forward secrecy.

**Reference:**

[OWASP Transport Layer Protection Cheat Sheet](https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html)

**Proof Of Concept:** here



## SSLv2 Offered – Vulnerable to DROWN Attack

CVE-2016-0800  
CVE-2016-0703

**CVSS Score:** 5.9

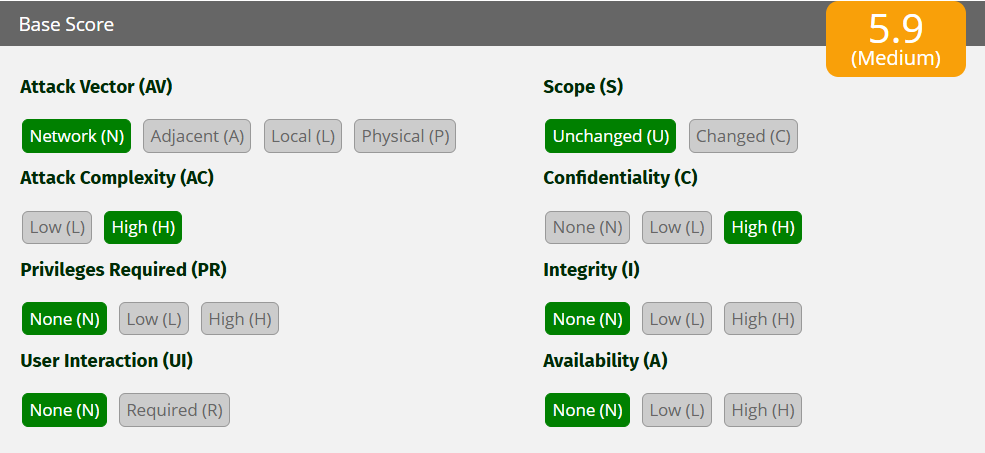
[Cite your source here.]

**CVE-ID**:

[Cite your source here.]

**Description**

**DROWN (Decrypting RSA with Obsolete and Weakened eNcryption)** is an attack that exploits **SSLv2** to decrypt TLS traffic. An attacker can launch a MitM attack and intercept encrypted communications, leading to information disclosure.



**Affected IP:** 20.239.145.15

**Affected Port:** TCP/443

**Technical Impact:**

**Man-in-the-Middle (MitM) Attack**

**Sensitive Data Disclosure** (e.g., passwords, session tokens, and financial data)

**Mitigation:**

**Disable SSLv2 entirely** on the server.

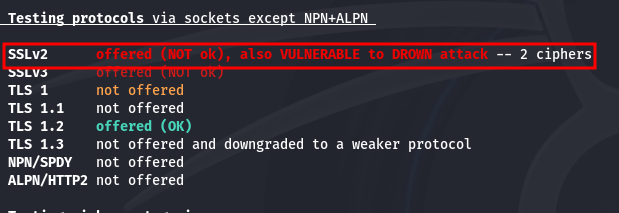
Use only **TLS 1.2 and TLS 1.3** protocols.

Apply patches for OpenSSL and server software.

**Reference:**

[CVE-2016-0800 – DROWN Attack](https://nvd.nist.gov/vuln/detail/CVE-2016-0800)

**Proof Of Concept:**



## Logjam Attack Vulnerability

**CVSS Score:** 5.9

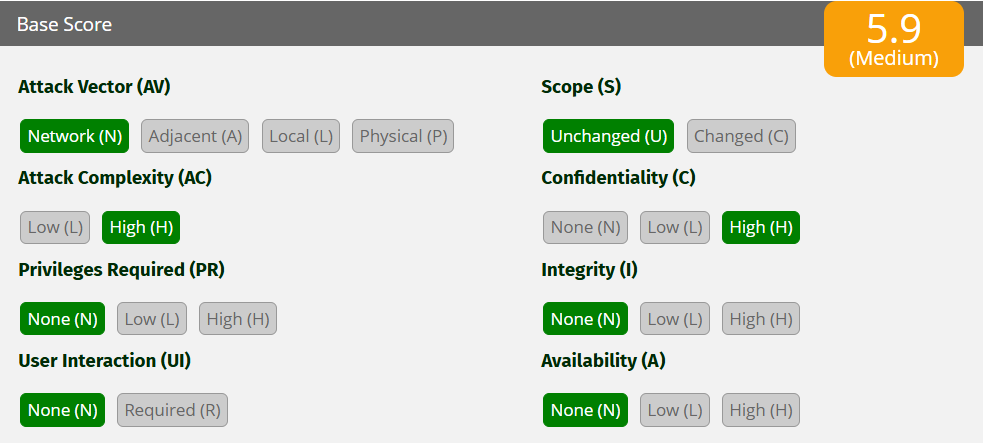
[Cite your source here.]

**CVE-ID**: CVE-2015-4000

[Cite your source here.]

**Description:**

**Logjam** targets **Diffie-Hellman (DH) key exchange** when **weak 1024-bit groups (Group 2)** are used. Attackers can downgrade the connection to a weaker cryptographic standard and decrypt encrypted traffic.



**Affected IP:** 20.239.145.15

**Affected Port:** TCP/443

**Technical Impact:**

**Man-in-the-Middle (MitM) Attack**

**Decryption of Encrypted Communication**

**Mitigation:**

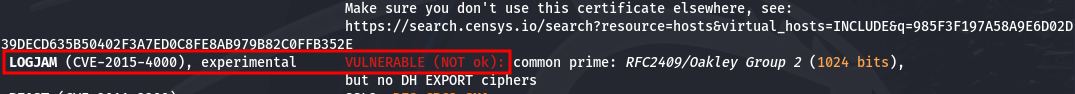
Use **2048-bit or higher Diffie-Hellman groups**.

Ensure that the server supports **Elliptic Curve Diffie-Hellman (ECDHE)** key exchange.

**Reference:**

[CVE-2015-4000 – Logjam Attack](https://nvd.nist.gov/vuln/detail/CVE-2015-4000)

**Proof Of Concept:**



## BREACH Attack Potential (Gzip HTTP Compression)

**CVSS Score:** 5.9

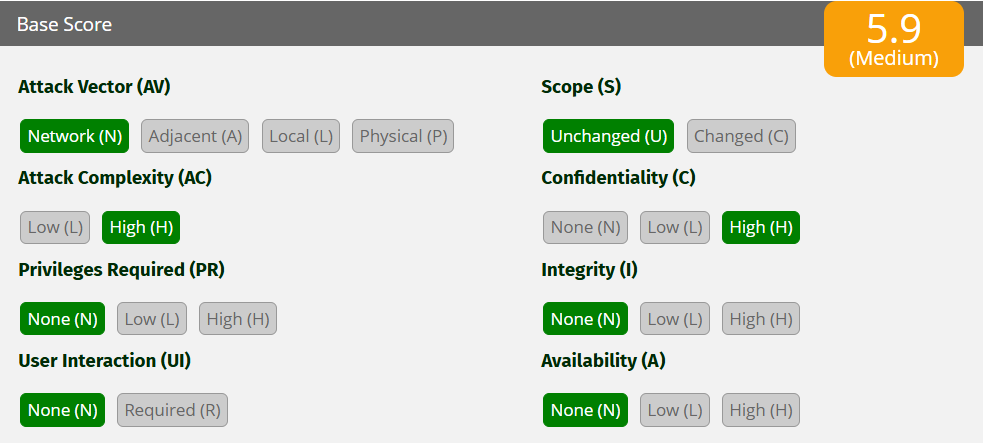
[Cite your source here.]

**CVE-ID**: CVE-2013-3587

[Cite your source here.]

**Description:**

**BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext)** is an attack that exploits **HTTP compression** (e.g., gzip) to steal sensitive data from HTTPS traffic



**Affected IP:** 20.239.145.15

**Affected Port:** TCP/443

**Technical Impact:**

**Data Leakage** (e.g., session cookies, CSRF tokens, etc.)

**Information Disclosure**

**Mitigation:**

**Disable HTTP compression** for responses containing sensitive data.

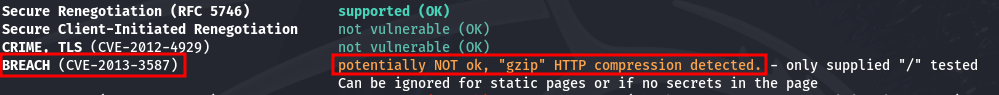
Use random padding to mitigate compression-based attacks.

Monitor for suspicious activity on compressed traffic.

**Reference:**

[CVE-2013-3587 – BREACH Attack](https://nvd.nist.gov/vuln/detail/CVE-2013-3587)

**Proof Of Concept:**



## Prometheus Node Exporter Directory Traversal

**CVSS Score:** 5.3

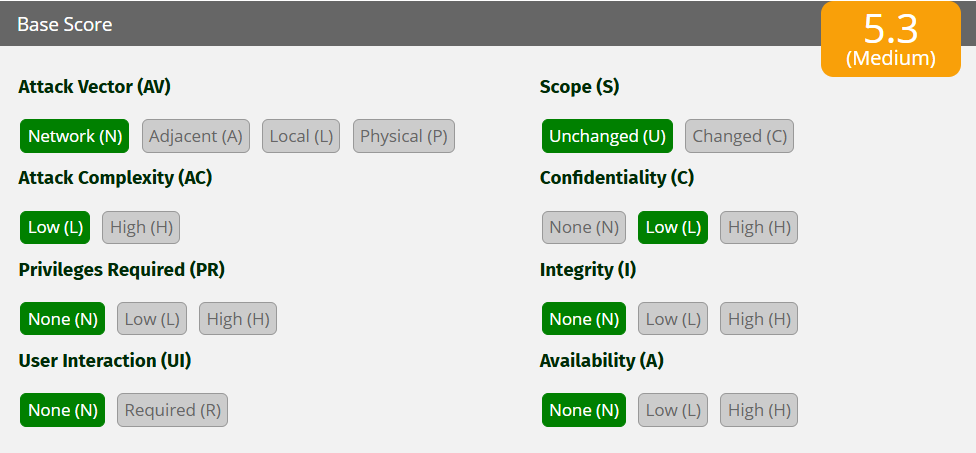
[Cite your source here.]

**CVE-ID**: CVE-2022-21698

[Cite your source here.]

**Description:**

The **Prometheus Node Exporter** exposes an endpoint (/metrics) for monitoring system metrics. Due to improper sanitization of input, this version is vulnerable to a **directory traversal attack**. Attackers can manipulate requests to access sensitive files such as **system logs, configuration files, and other data outside the intended directory**.



**Affected IP:** 184.164.141.29

**Affected Port:** TCP/9100

**Technical Impact:**

**Information Disclosure**: Attackers can access system files and logs, which may contain sensitive information.

**Reconnaissance**: The leaked data can be used for further attacks, such as privilege escalation or lateral movement.

**Security Bypass**: Potential exposure of passwords, private keys, and other critical information.

**Mitigation:**

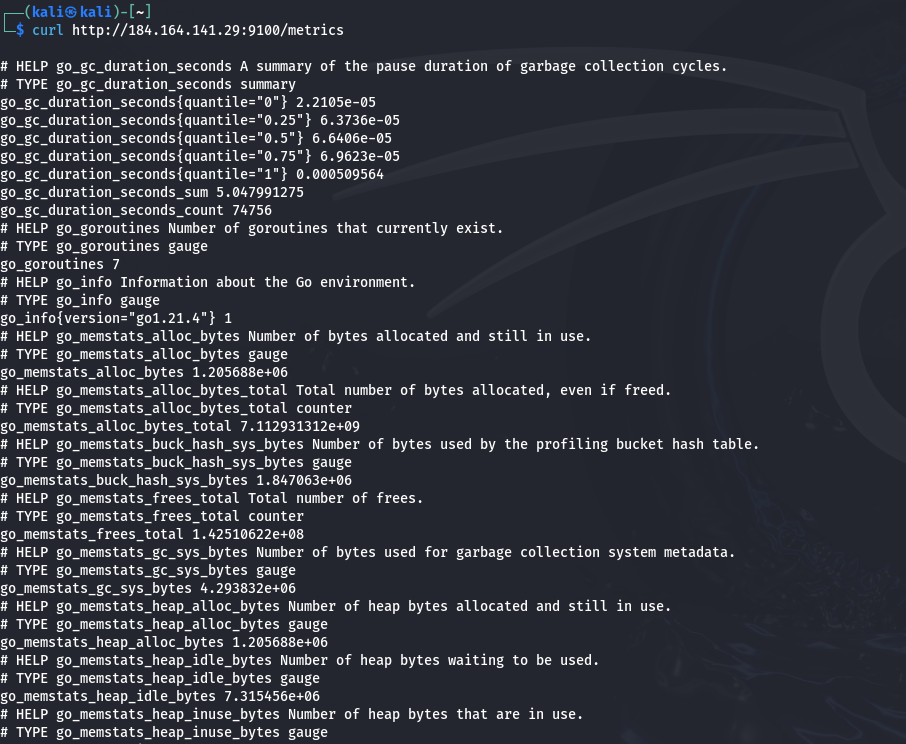
1. **Upgrade Prometheus Node Exporter to the latest version** (at least 1.7.2 or higher).
2. **Restrict access to port 9100** by using firewall rules. Allow connections only from trusted IP addresses.
3. Implement **authentication and encryption** (e.g., TLS) to protect the /metrics endpoint.
4. Regularly monitor logs for unauthorized access attempts.

**Reference:** https://

**Proof Of Concept:**

**Exploiting Directory Traversal:**  
Use a web browser or curl to send a crafted request to the Node Exporter’s /metrics endpoint

|  |
| --- |
| curl http://<target>:9100/metrics |



## Weak Cipher Suites

CVE-2013-2566

CVE-2015-2808

**CVSS Score:** 5.3

[Cite your source here.]

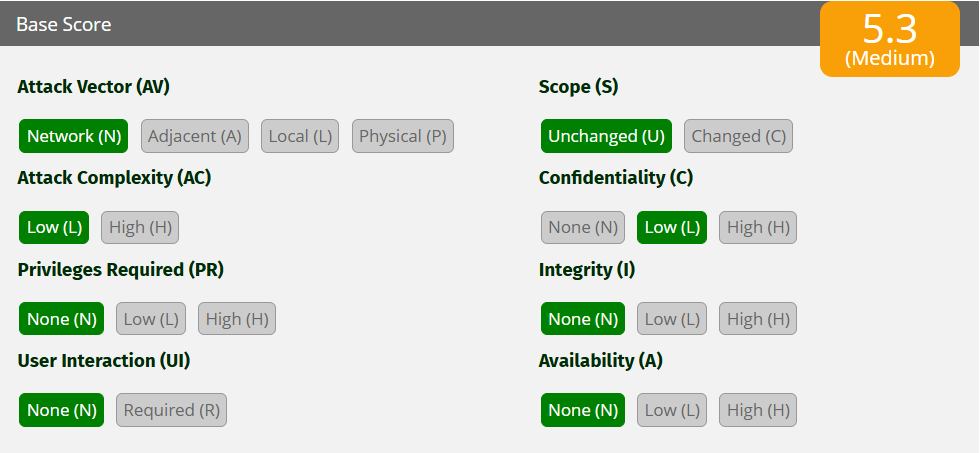
**Description:**

**CVE-ID**:

[Cite your source here.]

The server supports **RC4**, **3DES**, and **CBC-mode ciphers**, which are known to be insecure.

**RC4** is vulnerable to biases that allow attackers to decrypt traffic.



**Affected IP:** 47.241.101.3

**Affected Port:** TCP/50001

**Technical Impact:** **RC4** can be cracked in real-time by an attacker.

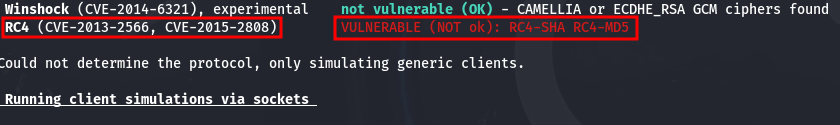
**Mitigation:**

Disable **RC4**, **3DES**, and **CBC-mode ciphers** in the server configuration.

Enforce the use of AES-GCM or ChaCha20-Poly1305 ciphers.

**Reference:**  RC4 Weakness

**Proof Of Concept:** here



## RC4 Cipher Vulnerability

**CVSS Score:** 4.3

[Cite your source here.]

**CVE-ID**: N/A

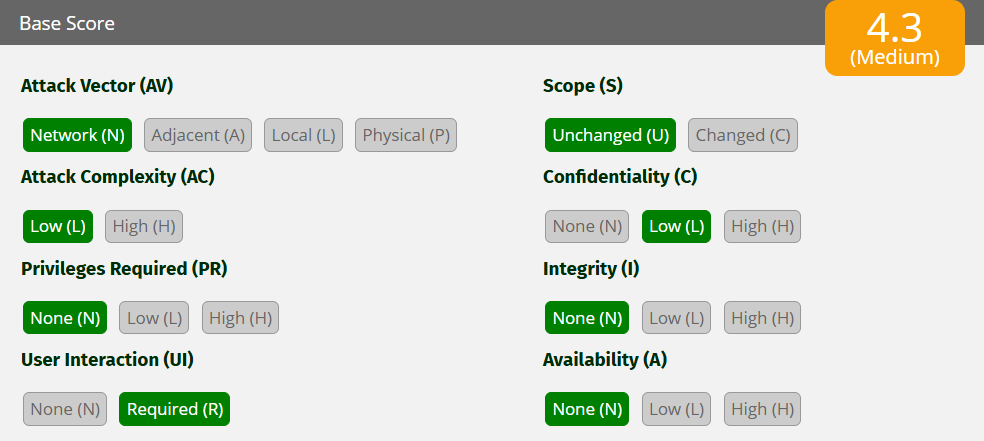
[Cite your source here.]

**Description:**

The server's certificate is **self-signed** and **not trusted**.

The **SAN (Subject Alternative Name) field is missing**, which is required in modern browsers.

No **OCSP (Online Certificate Status Protocol) or CRL (Certificate Revocation List)** information is available.



**Affected IP:**

47.241.101.3:50001

103.56.148.203:443

20.239.145.15:990

20.239.145.15:3389

**Affected Port:** TCP/50001, TCP/443. TCP/990, TCP/3389

**Technical Impact:**

Users receive a **certificate warning** when accessing the site.

MITM (Man-in-the-Middle) attacks are easier due to the lack of certificate validation.

**Mitigation:**

Obtain a valid SSL/TLS certificate from a trusted Certificate Authority (CA).

Ensure **SAN** is properly configured.

Enable **OCSP Stapling** and CRL checks.

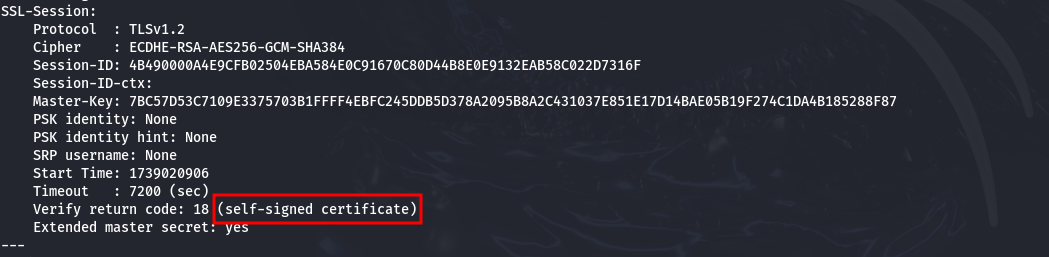
**Reference:**

[TLS Certificates Best Practices](https://letsencrypt.org/)

**Proof Of Concept:**

Check for self-signed certificate:

|  |
| --- |
| openssl s\_client -connect 47.241.101.3:50001 -showcerts |



## TLS\_FALLBACK\_SCSV Not Supported

CVE-2014-3566

CVE-2015-4000

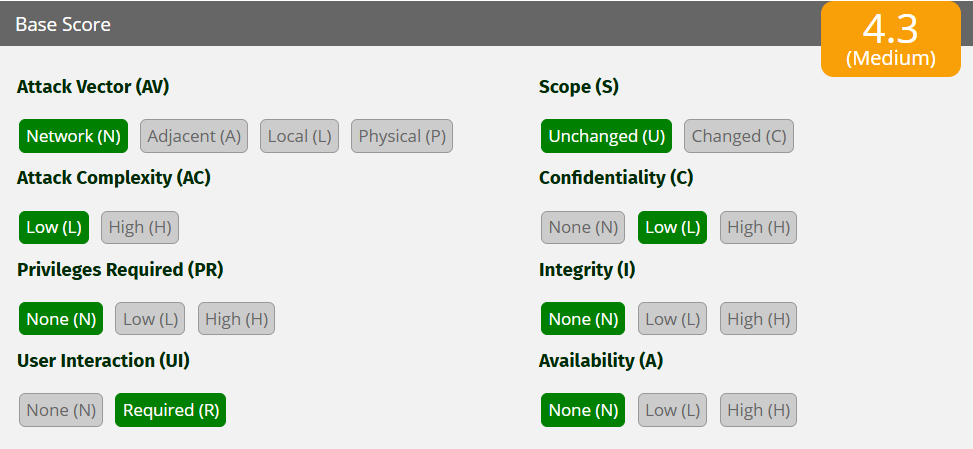
**CVE-ID**:

**CVSS Score:** 4.3

[Cite your source here.]

**Description:**

The server does **not support TLS\_FALLBACK\_SCSV**, which prevents protocol downgrade attacks.



**Affected IP:** 47.241.101.3

**Affected Port:** TCP/50001

**Technical Impact:**

Attackers can force connections to use weaker protocols (e.g., TLS 1.0).

**Mitigation:**

Enable **TLS\_FALLBACK\_SCSV** to prevent downgrade attacks.

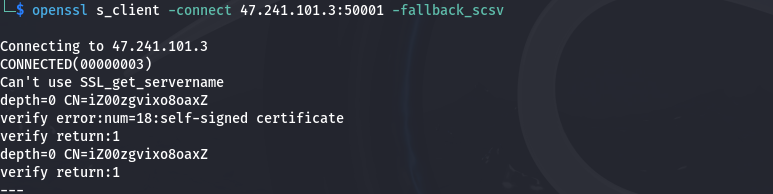
**Reference:**

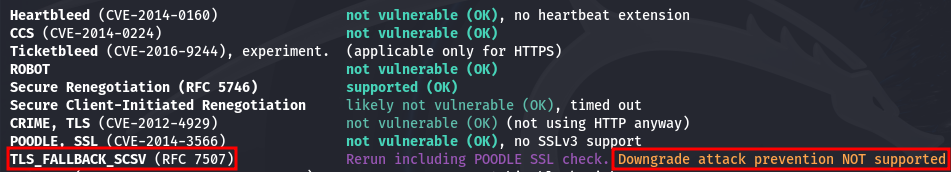
TLS\_FALLBACK\_SCSV

**Proof Of Concept:**

Check TLS downgrade prevention:

|  |
| --- |
| openssl s\_client -connect 47.241.101.3:50001 -fallback\_scsv |





# **LOW VULNERABILITES**

LOw VULNERABILITIES

## SSLv3 Offered – Vulnerable to POODLE Attack

**CVSS Score:** 3.7

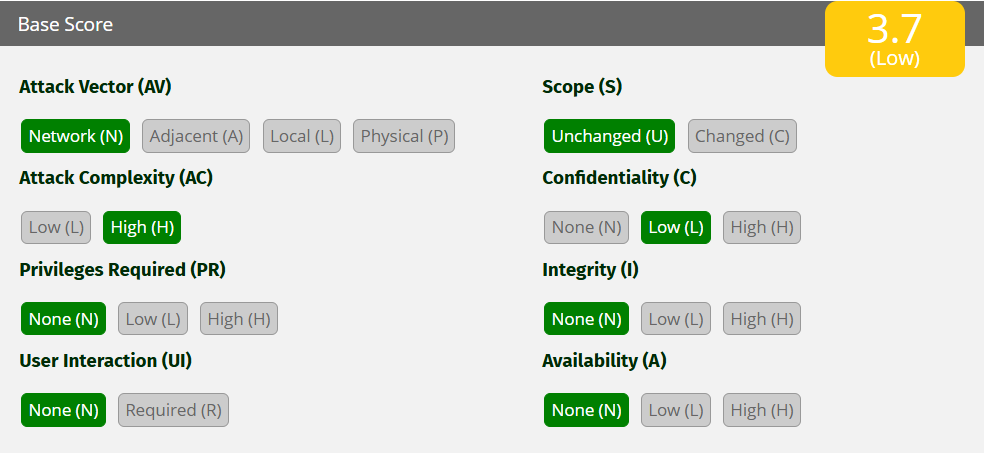
[Cite your source here.]

**CVE-ID**: CVE-2014-3566

[Cite your source here.]

**Description:**

**POODLE (Padding Oracle On Downgraded Legacy Encryption)** exploits padding flaws in **SSLv3**. Attackers can decrypt ciphertext and retrieve sensitive data, such as session cookies, from HTTPS traffic.



**Affected IP:** 20.239.145.15

**Affected Port:** TCP/443

**Technical Impact:**

**Data Decryption**

**Session Hijacking**

**Mitigation:**

**Disable SSLv3** on all services.

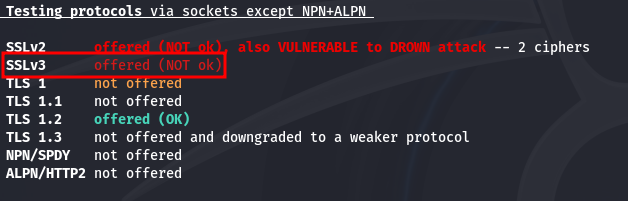
Ensure only **TLS 1.2 and TLS 1.3** are used.

Use **AEAD (Authenticated Encryption with Associated Data)** ciphers like AES-GCM.

**Reference:**

[CVE-2014-3566 – POODLE Attack](https://nvd.nist.gov/vuln/detail/CVE-2014-3566)

**Proof Of Concept:**



## SSL Sweet32 Attack- Birthday Attack

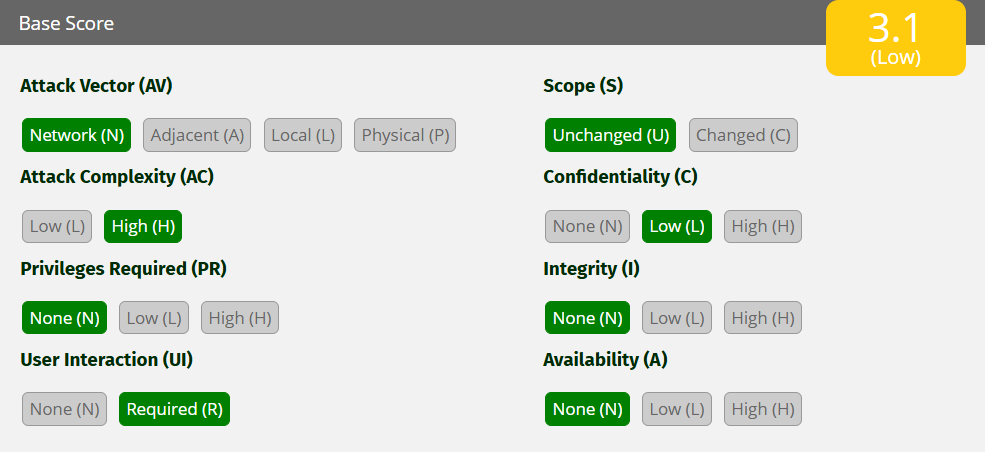
**CVSS Score:** 9.0

[Cite your source here.]

**Description:**   
 Sweet32 is a cryptographic attack that exploits the **birthday paradox** in 64-bit block ciphers like **3DES and Blowfish** used in **TLS, SSH, and VPNs**. Attackers can recover **parts of plaintext data (such as session cookies)** if they capture a Large amount of encrypted traffic.

**CVE-ID**: CVE-2016-2183

[Cite your source here.]



**Affected IP:** 47.241.101.3

**Affected Port:** TCP/50001

**Technical Impact:** Loss of Confidentiality

**Mitigation:** Upgrade

**Reference:**

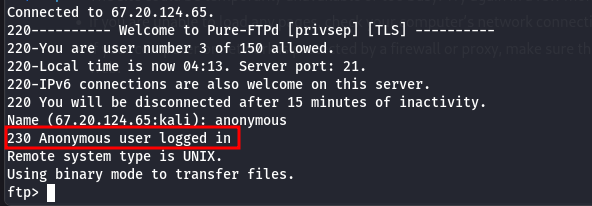
CVE-2016-2183-Sweet32 TLS Attack

<https://nvd.nist.gov/vuln/detail/CVE-2016-2183>

<https://sweet32.info/>

<https://access.redhat.com/security/cve/CVE-2016-2183>

**Proof Of Concept:** here



## Lucky13 Attack

**CVSS Score:** 2.1

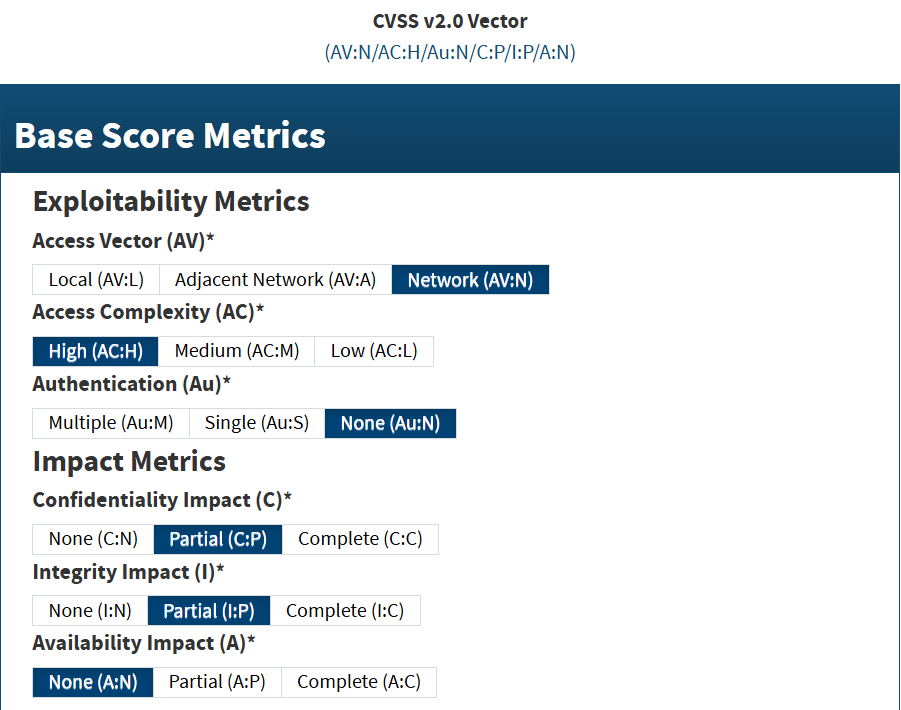
[Cite your source here.]

**Description:**

**CVE-ID**: CVE-2013-0169

[Cite your source here.]

Lucky13 is a padding oracle attack on **CBC-mode ciphers** in TLS.



**Affected IP:** 106.225.244.11

103.56.148.203

47.108.37.191

**Affected Port:** TCP/23, TCP/443

**Technical Impact:**

Allows decryption of encrypted communications through a timing attack.

**Mitigation:**

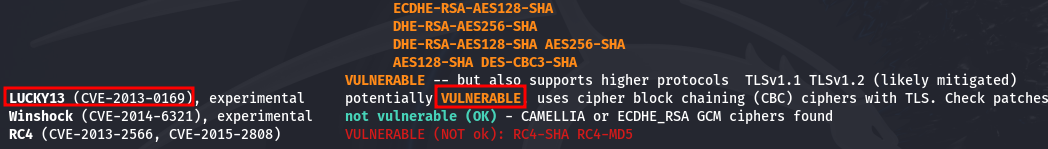
Disable **CBC-mode ciphers** and enforce AES-GCM.

**Reference:**

[Lucky13 Attack](https://docs.veracode.com/r/prevent-ssl-lucky13#:~:text=The%20SSL%20LUCKY13%20is%20a,in%2Dthe%2Dmiddle%20attack.)

**Proof Of Concept:**

Check for CBC ciphers:



# APPENDIX A - TOOLS USED

|  |  |
| --- | --- |
| **TOOL** | **DESCRIPTION** |
| **BurpSuite Community Edition** | Used for testing of web applications. |
| **Metasploit** | Used for exploitation of vulnerable services and vulnerability scanning. |
| **Nmap** | Used for scanning ports on hosts. |
| **Nikto** | Used for scanning web servers for security vulnerabilities. |
| **Sqlmap** | Used for detecting and exploiting SQL injection vulnerabilities. |
| **Dirb** | Used for web content discovery through brute-force directory scanning. |
| **Wireshark** | Used for network traffic analysis and packet sniffing |
| **Hydra** | Used for brute-force attacks on various authentication services. |
| **Testssl** | Used for testing SSL/TLS configurations and detecting vulnerabilities in encrypted connections |

***Table A.1:*** *Tools used during assessment*

# APPENDIX B - ENGAGEMENT INFORMATION

## Client Information

|  |  |
| --- | --- |
| **Client** | SURE TRUST |
| **Primary Contact** | NISHCHAY GABA Penetration Testing Trainer |
| **Approvers** | The following people are authorized to change the scope of engagement and modify the terms of the engagement   * NISHCHAY GABA * RADHA KUMARI (SURE TRUST head) |

## Version Information

|  |  |  |
| --- | --- | --- |
| **Version** | **Date** | **Description** |
| 1.0 | 09-02-2025 | Initial report to client |

## Contact Information

|  |  |
| --- | --- |
| **Name** | MUMMADI GOPAL VAMSI KRISHNA |
| **Address** | Maddilapalem, Visakhapatnam, Andhra Pradesh 530013 |
| **Phone** | +918184989401 |
| **Email** | Gopalvamsikrishnam1818@gmail.com |