IIJ Global

Sample Report

Vulnerability Assessment Report

PT. IIJ Global Solutions Indonesia

CONFIDENTIAL. This document is for internal purpose only.

Table of Contents

Executive Summary

This report is the result of Vulnerability Assessment that has been done by PT IIJGS Indonesia using Whitebox methodologies from the internet network.

This Vulnerability Assessment test overview:

Attackers look for so-called weak points and target them to launch attacks. Finding and improving an organization's weaknesses can be an effective defence strategy. This service analyses your organization's weaknesses that can be seen from outside the Internet and evaluates the security level.

The results have identified 4 Critical, 21 High, 6 Medium, and 0 Low vulnerability that require immediate attention to ensure the safety and integrity of the organization's systems and data.

No.	Finding Name	Affected Endpoint	CVSS Score	Status
Critical				
1	Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	10	Closed
2	Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5813-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	10	Closed
3	OpenSSL 3.0.0 < 3.0.3 Multiple Vulnerabilities	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	9.8	Closed
4	OpenSSL 3.0.0 < 3.0.4 Vulnerability	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	9.8	Closed
High				
5	Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	8.8	Closed
6	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	8.8	Closed
7	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5874-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	8.8	Closed

8	Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-5982-1)	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	8.8	Closed
9	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	7.8	Closed
10	Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6 5. 192.168.30.2 6. 192.168.30.3	7.8	Closed
11	Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6 5. 192.168.30.2 6. 192.168.30.3 7. 192.168.30.4 8. 192.178.30.5 9. 192.178.30.6	7.8	Closed
12	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6 5. 192.168.30.2 6. 192.168.30.3 7. 192.168.30.4	7.8	Closed
13	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5917-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6	7.8	Closed
14	Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6 5. 192.168.30.2 6. 192.168.30.3 7. 192.168.30.4	7.8	Closed
15	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6 5. 192.168.30.2 6. 192.168.30.3	7.8	Closed

16	Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)	1. 192.168.20.2 2.192.168.20.3 3.192.168.40.5 4. 192.168.40.6 5. 192.168.30.2 6. 192.168.30.3 7. 192.168.30.4	7.8	Closed
17	Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6044-1)	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.8	Closed
18	Ubuntu 20.04 LTS / 22.04 LTS / 22.10 : Linux kernel vulnerabilities (USN-6127-1)	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.8	Closed
19	Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6025-1)	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.8	Closed
20	Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6246-1)	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.8	Closed
21	Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6080-1)	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.8	Closed
22	OpenSSL 3.0.0 < 3.0.7 Multiple Vulnerabilities	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.5	Closed
23	OpenSSL 3.0.0 < 3.0.6 Vulnerability	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.5	Closed
24	OpenSSL 3.0.0 < 3.0.8 Multiple Vulnerabilities	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	7.4	Closed
25	Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6284-1)	1. 192.168.30.7	6.7	Closed
Medium				
26	SSL Certificate Cannot Be Trusted	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	6.5	Closed
27	SSL Self-Signed Certificate	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	6.5	Closed
28	Network Time Protocol (NTP) Mode 6 Scanner	1. 220.100.160.241 2. 220.100.160.242	5.8	Closed
29	OpenSSL 3.0.0 < 3.0.9 Multiple Vulnerabilities	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	5.3	Closed

30	OpenSSL 3.0.0 < 3.0.10 Multiple Vulnerabilities	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	5.3	Closed
31	OpenJDK 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1 Multiple Vulnerabilities (2023-01-17	1. 192.168.40.2 2. 192.168.40.3 3. 192.168.40.4	5.3	Closed

Preliminary

Background

- To make sure the infrastructure used for Monitoring customer already saved from attacker

Scope

Vulnerability Assessment test will target 16 IPs addresses.

1. 103.93.130.20 – Development server
2. 192.168.20.2 – main server 1
3. 192.168.20.3 – main server 2
4. 192.168.40.2 – elastic server 1
5. 192.168.40.3 – elastic server 2
6. 192.168.40.4 – elastic server 3
7. 192.168.40.5 – file server 1
8. 192.168.40.6 – file server 2
9. 192.168.30.2 – tenant server 1a
10. 192.168.30.3 – tenant server 1b
11. 192.168.30.4 – tenant server 2a
12. 192.168.30.5 – tenant server 2b
13. 192.168.30.6 – tenant server 3
14. 192.168.30.7 – tenant server 4
15. 220.100.160.241 – pfsense 2
16. 220.100.160.242 – pfsense 1

Methodology

Vulnerability assessment is a critical security testing methodology used to identify weaknesses in an organization's systems, networks, and applications.

Methodology for Vulnerability Assessment:

1. Planning and Scoping: Define the scope of the assessment and identify the systems, networks, and applications to be tested.
2. Information Gathering: Collect information about the systems, including IP addresses, network maps, and application details.
3. Vulnerability Scanning: Conduct automated scanning of the systems to identify known vulnerabilities.
4. Vulnerability Analysis: Evaluate the vulnerabilities identified in the scanning phase and determine their potential impact on the organization's security posture.
5. Reporting: Produce a report that documents the vulnerabilities found, their risk level, and recommended remediation steps.

Risk Scoring

Assessment of risk and the impact of security vulnerabilities found in the system is measured using CVSS (Common Vulnerability Scoring System). CVSS is an openly designed and standardized security vulnerability assessment system. CVSS can help PT YKK AP Indonesia to determine the priority for handling information security risks.

Severity Risk	Explanations	CVSS Score
Critical	An attacker can easily take over the host. This level of severity can cause compromise across your infrastructure network, “read” and “write” access to a file, and backdoors, and execute commands remotely.	9.0 – 10.0
High	An attacker can gain control of the host and cause leakage of highly sensitive information, access full “read” and “write” of a file, backdoors, and get a list of users on a host.	7.1 – 9.0
Medium	An attacker can get access to information specific to the host, including the security configuration that is in it. This has potential for host abuse. These severity level include access to files on a host, directory browsing, filtering rules from security configuration, denial of service attacks, and service usage by parties who do not have authorization such as mail-relaying	3.8 – 7.0
Low	An attacker can collect sensitive information such as the version of software installed. With this information, the attacker can easily exploit the vulnerability of software version	0.1 – 3.7
Informational	An attacker can collect information about host (open ports, services, etc.) and use this information to find another vulnerability.	0.0

Finding Discovered

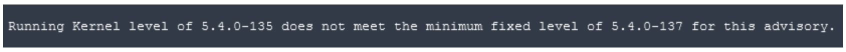
Production Server

192.168.20.2 – Main Server 1

Host Information

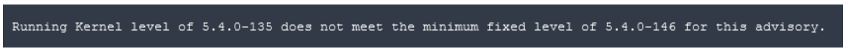
IP:	192.168.20.2
OS:	Ubuntu 20.04

Finding

Severity	Critical
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1) 2. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5813-1)
Description	1. The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5804-1 advisory. https://ubuntu.com/security/notices/USN-5804-1 2. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5813-1 advisory. https://ubuntu.com/security/notices/USN-5813-1
CVSS Score	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`
Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-137 for this advisory.`
Recommendation	Update the affected kernel package

Severity	High
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1) 2. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1) 3. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5874-1) 4. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1) 5. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1) 6. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities

	(USN-6251-1) 7. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) 8. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5917-1) 9. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 10. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1) 11. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)
Description	1. The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5980-1 advisory. https://ubuntu.com/security/notices/USN-5980-1 2. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5853-1 advisory. https://ubuntu.com/security/notices/USN-5853-1 3. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5874-1 advisory. https://ubuntu.com/security/notices/USN-5874-1 4. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5791-1 advisory. https://ubuntu.com/security/notices/USN-5791-1 5. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6047-1 advisory. https://ubuntu.com/security/notices/USN-6047-1 6. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 7. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory. https://ubuntu.com/security/notices/USN-6131-1 8. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5917-1 advisory. https://ubuntu.com/security/notices/USN-5917-1 9. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1

	https://ubuntu.com/security/notices/USN-6193-1 10. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory. https://ubuntu.com/security/notices/USN-6027-1 11. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory. https://ubuntu.com/security/notices/USN-6094-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`
Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-146 for this advisory.`
Recommendation	Update the affected kernel package

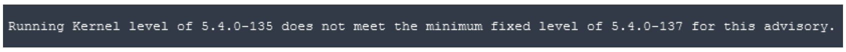
192.168.20.3 – Main Server 2

Host Information

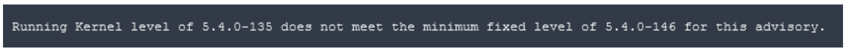
IP:	192.168.20.3
OS:	Ubuntu 20.04

Finding

Severity	Critical
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1) 2. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5813-1)
Description	1. The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5804-1 advisory. https://ubuntu.com/security/notices/USN-5804-1 2. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5813-1 advisory. https://ubuntu.com/security/notices/USN-5813-1
CVSS Score	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`

Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-137 for this advisory.`
Recommendation	Update the affected kernel package

Severity	High
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1) 2. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1) 3. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5874-1) 4. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1) 5. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1) 6. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) 7. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) 8. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5917-1) 9. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 10. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1) 11. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)
Description	1. The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5980-1 advisory. https://ubuntu.com/security/notices/USN-5980-1 2. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5853-1 advisory. https://ubuntu.com/security/notices/USN-5853-1 3. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5874-1 advisory. https://ubuntu.com/security/notices/USN-5874-1 4. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5791-1 advisory. https://ubuntu.com/security/notices/USN-5791-1 5. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as

	referenced in the USN-6047-1 advisory. https://ubuntu.com/security/notices/USN-6047-1 6. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 7. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory. https://ubuntu.com/security/notices/USN-6131-1 8. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5917-1 advisory. https://ubuntu.com/security/notices/USN-5917-1 9. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 10. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory. https://ubuntu.com/security/notices/USN-6027-1 11. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory. https://ubuntu.com/security/notices/USN-6094-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`
Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-146 for this advisory.`
Recommendation	Update the affected kernel package

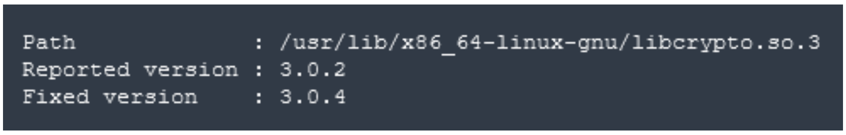
192.168.40.2 – elastic server 1

Host Information

IP: 192.168.40.2
OS: Ubuntu 20.04

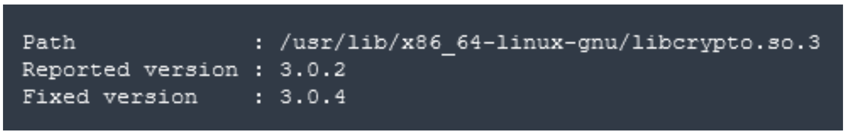
Finding

Severity	Critical
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.3 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.4 Vulnerability
Description	1. The version of OpenSSL installed on the remote host is prior to 3.0.3. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.3 advisory. https://cve.org/CVERecord?id=CVE-2022-1473 http://www.nessus.org/u?9131c964 https://www.openssl.org/news/secadv/20220503.txt https://cve.org/CVERecord?id=CVE-2022-1434 http://www.nessus.org/u?14b3b0bd https://cve.org/CVERecord?id=CVE-2022-1343 http://www.nessus.org/u?ee860149 https://cve.org/CVERecord?id=CVE-2022-1292 http://www.nessus.org/u?2d2d6fcb 2. The version of OpenSSL installed on the remote host is prior to 3.0.4. It is, therefore, affected by a vulnerability as referenced in the 3.0.4 advisory. https://cve.org/CVERecord?id=CVE-2022-2068 http://www.nessus.org/u?6569bd51 https://www.openssl.org/news/secadv/20220621.txt
CVSS Score	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Affected version	3.0.0

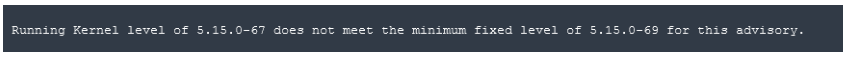
Evidence	
	`Path              : /usr/lib/x86_64-linux-gnu/libcrypto.so.3`
	`Reported version : 3.0.2`
	`Fixed version    : 3.0.4`

Recommendation	Upgrade to OpenSSL to the latest version

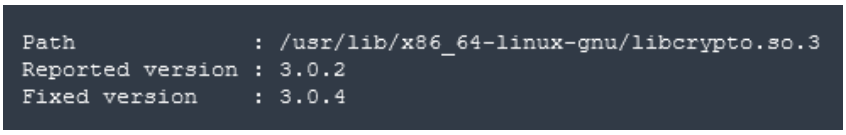
Severity	High
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.7 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.6 Vulnerability 3. OpenSSL 3.0.0 < 3.0.8 Multiple Vulnerabilities
Description	1. The version of OpenSSL installed on the remote host is prior to

	3.0.7. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.7 advisory. https://www.openssl.org/news/secadv/20221101.txt http://www.nessus.org/u?a438010d 2. The version of OpenSSL installed on the remote host is prior to 3.0.6. It is, therefore, affected by a vulnerability as referenced in the 3.0.6 advisory. https://cve.org/CVERecord?id=CVE-2022-3358 http://www.nessus.org/u?87748528d https://www.openssl.org/news/secadv/20221011.txt 3. The version of OpenSSL installed on the remote host is prior to 3.0.8. It is, therefore, affected by a denial of service (DoS) vulnerability. If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the -policy argument to the command line utilities or by calling either X509_VERIFY_PARAM_add0_policy() or X509_VERIFY_PARAM_set1_policies() functions. https://www.cve.org/CVERecord?id=CVE-2023-0401 https://www.openssl.org/news/secadv/20230207.txt https://www.openssl.org/policies/secpolicy.html https://www.cve.org/CVERecord?id=CVE-2023-0286 https://www.cve.org/CVERecord?id=CVE-2023-0217 https://www.cve.org/CVERecord?id=CVE-2023-0216 https://www.cve.org/CVERecord?id=CVE-2023-0215 https://www.cve.org/CVERecord?id=CVE-2022-4450 https://www.cve.org/CVERecord?id=CVE-2022-4304 https://www.cve.org/CVERecord?id=CVE-2022-4203
CVSS Score	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Affected version	3.0.0
Evidence	 Path : /usr/lib/x86_64-linux-gnu/libcrypto.so.3 Reported version : 3.0.2 Fixed version : 3.0.4
Recommendation	Upgrade to OpenSSL to the latest version

Severity	High
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-5982-1) 2. Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6044-1) 3. Ubuntu 20.04 LTS / 22.04 LTS / 22.10 : Linux kernel vulnerabilities (USN-6127-1) 4. Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6025-1) 5. Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6246-1) 6. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 7. Ubuntu 20.04 LTS / 22.04 LTS : Linux kernel vulnerabilities (USN-6080-1)
Description	1. The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5982-1 advisory. https://ubuntu.com/security/notices/USN-5982-1 2. The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6044-1 advisory. https://ubuntu.com/security/notices/USN-6044-1 3. The remote Ubuntu 20.04 LTS / 22.04 LTS / 22.10 host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6127-1 advisory. https://ubuntu.com/security/notices/USN-6127-1 4. The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6025-1 advisory. https://ubuntu.com/security/notices/USN-6025-1 5. The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6246-1 advisory. https://ubuntu.com/security/notices/USN-6246-1 6. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 7. The remote Ubuntu 20.04 LTS / 22.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6080-1 advisory. https://ubuntu.com/security/notices/USN-6080-1
CVSS Score	8.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
Affected kernel	`5.15.0-67`

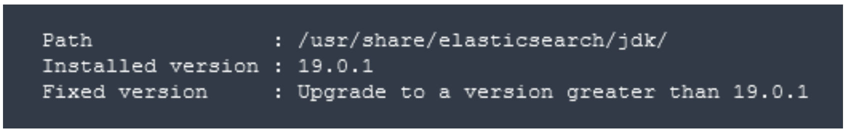
Evidence	 `Running Kernel level of 5.15.0-67 does not meet the minimum fixed level of 5.15.0-69 for this advisory.`
Recommendation	Update the affected kernel package.

Severity	**Medium**
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.9 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.10 Multiple Vulnerabilities
Description	1. The version of OpenSSL installed on the remote host is prior to 3.0.9. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.9 advisory. http://www.nessus.org/u?91a43679 https://www.cve.org/CVERecord?id=CVE-2023-0465 https://www.openssl.org/news/secadv/20230328.txt https://www.openssl.org/policies/secpolicy.html http://www.nessus.org/u?a5af6e0b https://www.cve.org/CVERecord?id=CVE-2023-0466 http://www.nessus.org/u?0fd4fada https://www.cve.org/CVERecord?id=CVE-2023-0464 https://www.openssl.org/news/secadv/20230322.txt 2. The version of OpenSSL installed on the remote host is prior to 3.0.10. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.10 advisory. http://www.nessus.org/u?92592957 http://www.nessus.org/u?e3173aec https://www.openssl.org/news/secadv/20230719.txt https://www.openssl.org/news/secadv/20230731.txt https://www.openssl.org/policies/secpolicy.html http://www.nessus.org/u?a7b15686 https://www.openssl.org/news/secadv/20230714.txt https://www.cve.org/CVERecord?id=CVE-2023-2975 https://www.cve.org/CVERecord?id=CVE-2023-3446 https://www.cve.org/CVERecord?id=CVE-2023-3817
CVSS Score	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected version	`3.0.0`

Evidence	
	`Path             : /usr/lib/x86_64-linux-gnu/libcrypto.so.3`
	`Reported version : 3.0.2`
	`Fixed version    : 3.0.4`

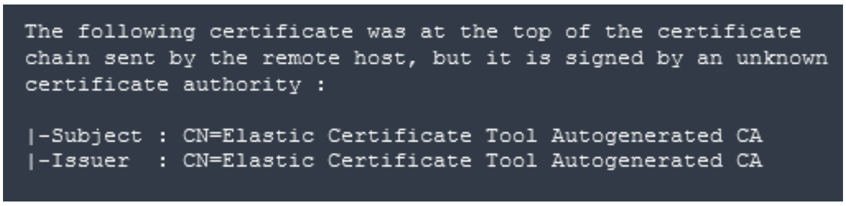
Recommendation	Upgrade to OpenSSL to the latest version

Severity	Medium
Name	OpenJDK 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1 Multiple Vulnerabilities (2023-01-17
Description	The version of OpenJDK installed on the remote host is prior to 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the 2023-01-17 advisory. https://openjdk.java.net/groups/vulnerability/advisories/2023-01-17
CVSS Score	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected version	`19.0.1`

Evidence	
	`Path              : /usr/share/elasticsearch/jdk/`
	`Installed version : 19.0.1`
	`Fixed version     : Upgrade to a version greater than 19.0.1`

Recommendation	Upgrade to an OpenJDK version greater than 7u361 / 8u352 / 11.0.17 / 13.0.13 / 15.0.9 / 17.0.5 / 19.0.1

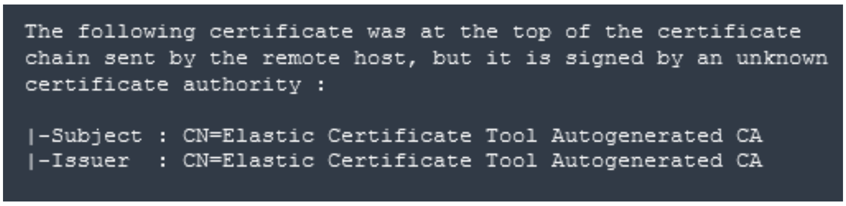
Severity	Medium
Name	SSL Certificate Cannot Be Trusted
Description	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken. https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
CVSS Score	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Affected port	`9200`

Evidence	
	`The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :`
	
	`|-Subject  : CN=Elastic Certificate Tool Autogenerated CA`
	`|-Issuer   : CN=Elastic Certificate Tool Autogenerated CA`

Recommendation	Purchase or generate a proper SSL certificate for this service.

Severity	Medium
Name	SSL Self-Signed Certificate

Description	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
CVSS Score	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Affected port	`9200`

Evidence	
	`The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :`
	`|-Subject : CN=Elastic Certificate Tool Autogenerated CA`
	`|-Issuer  : CN=Elastic Certificate Tool Autogenerated CA`

Recommendation	Purchase or generate a proper SSL certificate for this service.

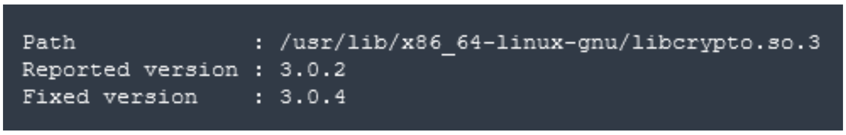
192.168.40.3 – elastic server 2

Host Information

IP: 192.168.40.3
OS: Ubuntu 20.04

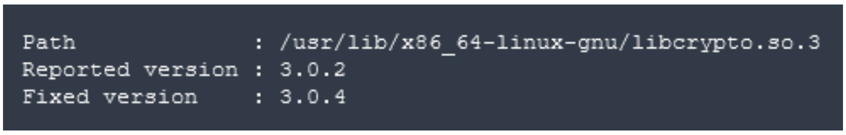
Finding

Severity	**Critical**
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.3 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.4 Vulnerability
Description	1. The version of OpenSSL installed on the remote host is prior to 3.0.3. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.3 advisory. https://cve.org/CVERecord?id=CVE-2022-1473 http://www.nessus.org/u?9131c964 https://www.openssl.org/news/secadv/20220503.txt https://cve.org/CVERecord?id=CVE-2022-1434 http://www.nessus.org/u?14b3b0bd https://cve.org/CVERecord?id=CVE-2022-1343 http://www.nessus.org/u?ee860149 https://cve.org/CVERecord?id=CVE-2022-1292 http://www.nessus.org/u?2d2d6fcb 2. The version of OpenSSL installed on the remote host is prior to 3.0.4. It is, therefore, affected by a vulnerability as referenced in the 3.0.4 advisory. https://cve.org/CVERecord?id=CVE-2022-2068 http://www.nessus.org/u?6569bd51 https://www.openssl.org/news/secadv/20220621.txt
CVSS Score	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Affected version	`3.0.0`

Evidence	
	`Path             : /usr/lib/x86_64-linux-gnu/libcrypto.so.3`
	`Reported version : 3.0.2`
	`Fixed version    : 3.0.4`

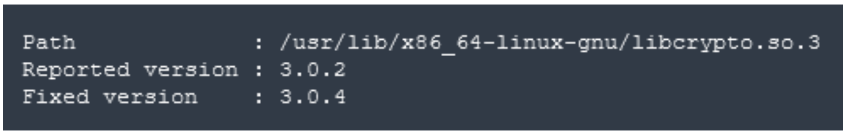
Recommendation	Upgrade to OpenSSL to the latest version

Severity	**High**
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.7 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.6 Vulnerability 3. OpenSSL 3.0.0 < 3.0.8 Multiple Vulnerabilities
Description	1. The version of OpenSSL installed on the remote host is prior to

	3.0.7. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.7 advisory. https://www.openssl.org/news/secadv/20221101.txt http://www.nessus.org/u?a438010d 2. The version of OpenSSL installed on the remote host is prior to 3.0.6. It is, therefore, affected by a vulnerability as referenced in the 3.0.6 advisory. https://cve.org/CVERecord?id=CVE-2022-3358 http://www.nessus.org/u?87748528d https://www.openssl.org/news/secadv/20221011.txt 3. The version of OpenSSL installed on the remote host is prior to 3.0.8. It is, therefore, affected by a denial of service (DoS) vulnerability. If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the -policy argument to the command line utilities or by calling either X509_VERIFY_PARAM_add0_policy() or X509_VERIFY_PARAM_set1_policies() functions. https://www.cve.org/CVERecord?id=CVE-2023-0401 https://www.openssl.org/news/secadv/20230207.txt https://www.openssl.org/policies/secpolicy.html https://www.cve.org/CVERecord?id=CVE-2023-0286 https://www.cve.org/CVERecord?id=CVE-2023-0217 https://www.cve.org/CVERecord?id=CVE-2023-0216 https://www.cve.org/CVERecord?id=CVE-2023-0215 https://www.cve.org/CVERecord?id=CVE-2022-4450 https://www.cve.org/CVERecord?id=CVE-2022-4304 https://www.cve.org/CVERecord?id=CVE-2022-4203
CVSS Score	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Affected version	3.0.0
Evidence	 Path : /usr/lib/x86_64-linux-gnu/libcrypto.so.3 Reported version : 3.0.2 Fixed version : 3.0.4
Recommendation	Upgrade to OpenSSL to the latest version

Severity	**Medium**
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.9 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.10 Multiple Vulnerabilities

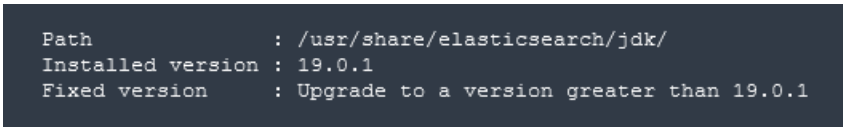
Description	1. The version of OpenSSL installed on the remote host is prior to 3.0.9. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.9 advisory. http://www.nessus.org/u?91a43679 https://www.cve.org/CVERecord?id=CVE-2023-0465 https://www.openssl.org/news/secadv/20230328.txt https://www.openssl.org/policies/secpolicy.html http://www.nessus.org/u?a5af6e0b https://www.cve.org/CVERecord?id=CVE-2023-0466 http://www.nessus.org/u?0fd4fada https://www.cve.org/CVERecord?id=CVE-2023-0464 https://www.openssl.org/news/secadv/20230322.txt 2. The version of OpenSSL installed on the remote host is prior to 3.0.10. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.10 advisory. http://www.nessus.org/u?92592957 http://www.nessus.org/u?e3173aec https://www.openssl.org/news/secadv/20230719.txt https://www.openssl.org/news/secadv/20230731.txt https://www.openssl.org/policies/secpolicy.html http://www.nessus.org/u?a7b15686 https://www.openssl.org/news/secadv/20230714.txt https://www.cve.org/CVERecord?id=CVE-2023-2975 https://www.cve.org/CVERecord?id=CVE-2023-3446 https://www.cve.org/CVERecord?id=CVE-2023-3817
CVSS Score	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected version	`3.0.0`

Evidence	
	`Path              : /usr/lib/x86_64-linux-gnu/libcrypto.so.3`
	`Reported version : 3.0.2`
	`Fixed version    : 3.0.4`

Recommendation	Upgrade to OpenSSL to the latest version

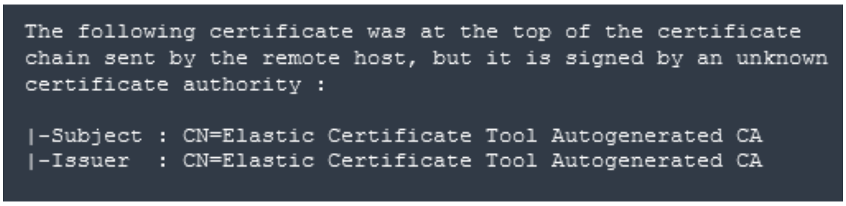
Severity	**Medium**
Name	OpenJDK 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1 Multiple Vulnerabilities (2023-01-17
Description	The version of OpenJDK installed on the remote host is prior to 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the 2023-01-17 advisory. https://openjdk.java.net/groups/vulnerability/advisories/2023-01-17

CVSS Score	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected version	`19.0.1`

Evidence	
	`Path              : /usr/share/elasticsearch/jdk/`
	`Installed version : 19.0.1`
	`Fixed version     : Upgrade to a version greater than 19.0.1`

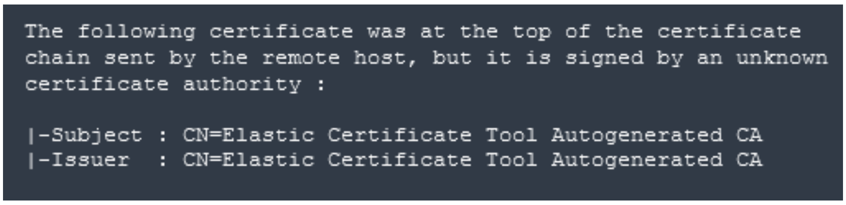
Recommendation	Upgrade to an OpenJDK version greater than 7u361 / 8u352 / 11.0.17 / 13.0.13 / 15.0.9 / 17.0.5 / 19.0.1

Severity	**Medium**
Name	SSL Certificate Cannot Be Trusted
Description	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken. https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
CVSS Score	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Affected port	`9200`

Evidence	
	`The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :`
	
	`|-Subject  : CN=Elastic Certificate Tool Autogenerated CA`
	`|-Issuer   : CN=Elastic Certificate Tool Autogenerated CA`

Recommendation	Purchase or generate a proper SSL certificate for this service.

Severity	**Medium**
Name	SSL Self-Signed Certificate
Description	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
CVSS Score	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Affected port	`9200`

Evidence	 The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority : |-Subject : CN=Elastic Certificate Tool Autogenerated CA |-Issuer : CN=Elastic Certificate Tool Autogenerated CA
Recommendation	Purchase or generate a proper SSL certificate for this service.

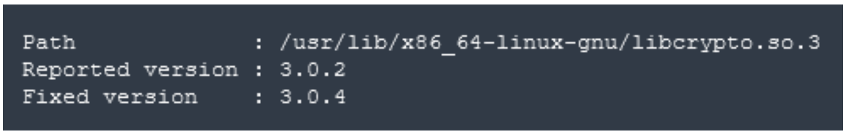
192.168.40.4 – elastic server 3

Host Information

IP:	192.168.40.4
OS:	Ubuntu 20.04

Finding

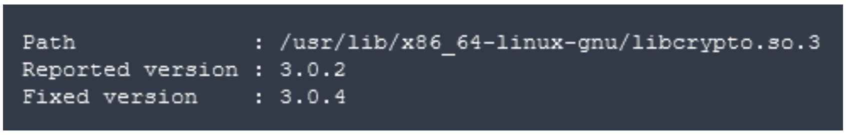
Severity	Critical
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.3 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.4 Vulnerability
Description	1. The version of OpenSSL installed on the remote host is prior to 3.0.3. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.3 advisory. https://cve.org/CVERecord?id=CVE-2022-1473 http://www.nessus.org/u?9131c964 https://www.openssl.org/news/secadv/20220503.txt https://cve.org/CVERecord?id=CVE-2022-1434 http://www.nessus.org/u?14b3b0bd https://cve.org/CVERecord?id=CVE-2022-1343 http://www.nessus.org/u?ee860149 https://cve.org/CVERecord?id=CVE-2022-1292 http://www.nessus.org/u?2d2d6fcb 2. The version of OpenSSL installed on the remote host is prior to 3.0.4. It is, therefore, affected by a vulnerability as referenced in the 3.0.4 advisory. https://cve.org/CVERecord?id=CVE-2022-2068 http://www.nessus.org/u?6569bd51 https://www.openssl.org/news/secadv/20220621.txt
CVSS Score	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Affected version	`3.0.0`

Evidence	
	`Path             : /usr/lib/x86_64-linux-gnu/libcrypto.so.3`
	`Reported version : 3.0.2`
	`Fixed version    : 3.0.4`

Recommendation	Upgrade to OpenSSL to the latest version

Severity	High
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.7 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.6 Vulnerability 3. OpenSSL 3.0.0 < 3.0.8 Multiple Vulnerabilities
Description	1. The version of OpenSSL installed on the remote host is prior to

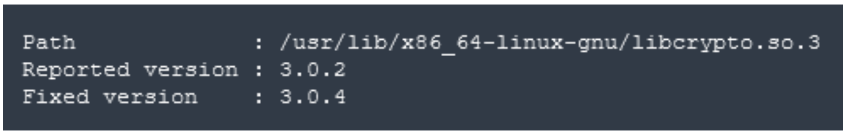
	3.0.7. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.7 advisory. https://www.openssl.org/news/secadv/20221101.txt http://www.nessus.org/u?a438010d 2. The version of OpenSSL installed on the remote host is prior to 3.0.6. It is, therefore, affected by a vulnerability as referenced in the 3.0.6 advisory. https://cve.org/CVERecord?id=CVE-2022-3358 http://www.nessus.org/u?87748528d https://www.openssl.org/news/secadv/20221011.txt 3. The version of OpenSSL installed on the remote host is prior to 3.0.8. It is, therefore, affected by a denial of service (DoS) vulnerability. If an X.509 certificate contains a malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. Policy processing being enabled on a publicly facing server is not considered to be a common setup. Policy processing is enabled by passing the -policy argument to the command line utilities or by calling either X509_VERIFY_PARAM_add0_policy() or X509_VERIFY_PARAM_set1_policies() functions. https://www.cve.org/CVERecord?id=CVE-2023-0401 https://www.openssl.org/news/secadv/20230207.txt https://www.openssl.org/policies/secpolicy.html https://www.cve.org/CVERecord?id=CVE-2023-0286 https://www.cve.org/CVERecord?id=CVE-2023-0217 https://www.cve.org/CVERecord?id=CVE-2023-0216 https://www.cve.org/CVERecord?id=CVE-2023-0215 https://www.cve.org/CVERecord?id=CVE-2022-4450 https://www.cve.org/CVERecord?id=CVE-2022-4304 https://www.cve.org/CVERecord?id=CVE-2022-4203
CVSS Score	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
Affected version	`3.0.0`

Evidence	
	`Path             : /usr/lib/x86_64-linux-gnu/libcrypto.so.3`
	`Reported version : 3.0.2`
	`Fixed version    : 3.0.4`

Recommendation	Upgrade to OpenSSL to the latest version

Severity	**Medium**
Name	Multiple Vulnerability on OpenSSL 1. OpenSSL 3.0.0 < 3.0.9 Multiple Vulnerabilities 2. OpenSSL 3.0.0 < 3.0.10 Multiple Vulnerabilities

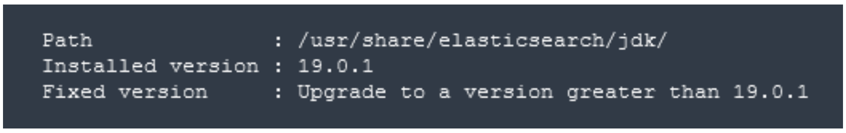
Description	1. The version of OpenSSL installed on the remote host is prior to 3.0.9. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.9 advisory. http://www.nessus.org/u?91a43679 https://www.cve.org/CVERecord?id=CVE-2023-0465 https://www.openssl.org/news/secadv/20230328.txt https://www.openssl.org/policies/secpolicy.html http://www.nessus.org/u?a5af6e0b https://www.cve.org/CVERecord?id=CVE-2023-0466 http://www.nessus.org/u?0fd4fada https://www.cve.org/CVERecord?id=CVE-2023-0464 https://www.openssl.org/news/secadv/20230322.txt 2. The version of OpenSSL installed on the remote host is prior to 3.0.10. It is, therefore, affected by multiple vulnerabilities as referenced in the 3.0.10 advisory. http://www.nessus.org/u?92592957 http://www.nessus.org/u?e3173aec https://www.openssl.org/news/secadv/20230719.txt https://www.openssl.org/news/secadv/20230731.txt https://www.openssl.org/policies/secpolicy.html http://www.nessus.org/u?a7b15686 https://www.openssl.org/news/secadv/20230714.txt https://www.cve.org/CVERecord?id=CVE-2023-2975 https://www.cve.org/CVERecord?id=CVE-2023-3446 https://www.cve.org/CVERecord?id=CVE-2023-3817
CVSS Score	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected version	`3.0.0`

Evidence	
	`Path             : /usr/lib/x86_64-linux-gnu/libcrypto.so.3`
	`Reported version : 3.0.2`
	`Fixed version    : 3.0.4`

Recommendation	Upgrade to OpenSSL to the latest version

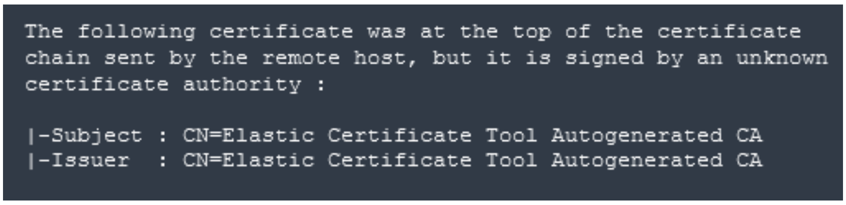
Severity	**Medium**
Name	OpenJDK 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <= 15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1 Multiple Vulnerabilities (2023-01-17
Description	The version of OpenJDK installed on the remote host is prior to 7 <= 7u361 / 8 <= 8u352 / 11.0.0 <= 11.0.17 / 13.0.0 <= 13.0.13 / 15.0.0 <=

	15.0.9 / 17.0.0 <= 17.0.5 / 19.0.0 <= 19.0.1. It is, therefore, affected by multiple vulnerabilities as referenced in the 2023-01-17 advisory. https://openjdk.java.net/groups/vulnerability/advisories/2023-01-17
CVSS Score	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N)
Affected version	`19.0.1`

Evidence	
	`Path              : /usr/share/elasticsearch/jdk/`
	`Installed version : 19.0.1`
	`Fixed version     : Upgrade to a version greater than 19.0.1`

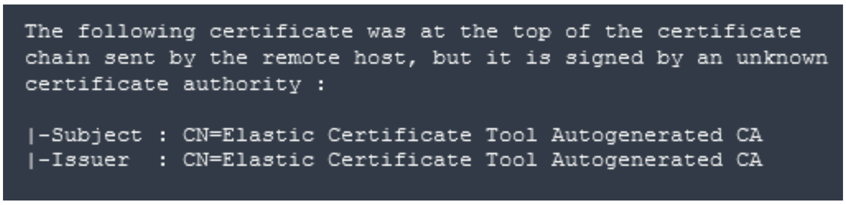
Recommendation	Upgrade to an OpenJDK version greater than 7u361 / 8u352 / 11.0.17 / 13.0.13 / 15.0.9 / 17.0.5 / 19.0.1

Severity	**Medium**
Name	SSL Certificate Cannot Be Trusted
Description	The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken. https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
CVSS Score	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Affected port	`9200`

Evidence	
	`The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority :`
	
	`|-Subject  : CN=Elastic Certificate Tool Autogenerated CA`
	`|-Issuer   : CN=Elastic Certificate Tool Autogenerated CA`

Recommendation	Purchase or generate a proper SSL certificate for this service.

Severity	**Medium**
Name	SSL Self-Signed Certificate
Description	The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
CVSS Score	6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)
Affected port	`9200`

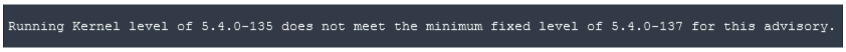
Evidence	 The following certificate was at the top of the certificate chain sent by the remote host, but it is signed by an unknown certificate authority : |-Subject : CN=Elastic Certificate Tool Autogenerated CA |-Issuer : CN=Elastic Certificate Tool Autogenerated CA
Recommendation	Purchase or generate a proper SSL certificate for this service.

192.168.40.5 – file server 1

Host Information

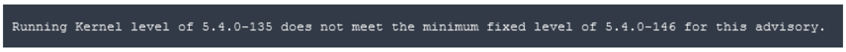
IP: 192.168.40.5
OS: Ubuntu 20.04

Finding

Severity	Critical
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1) 2. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5813-1)
Description	1. The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5804-1 advisory. https://ubuntu.com/security/notices/USN-5804-1 2. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5813-1 advisory. https://ubuntu.com/security/notices/USN-5813-1
CVSS Score	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`
Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-137 for this advisory.`
Recommendation	Update the affected kernel package

Severity	High
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1) 2. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1) 3. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5874-1) 4. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1) 5. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1) 6. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) 7. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) 8. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities

	(USN-5917-1) 9. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 10. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 11. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1) 12. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)
Description	1. The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5980-1 advisory. https://ubuntu.com/security/notices/USN-5980-1 2. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5853-1 advisory. https://ubuntu.com/security/notices/USN-5853-1 3. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5874-1 advisory. https://ubuntu.com/security/notices/USN-5874-1 4. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5791-1 advisory. https://ubuntu.com/security/notices/USN-5791-1 5. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6047-1 advisory. https://ubuntu.com/security/notices/USN-6047-1 6. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 7. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory. https://ubuntu.com/security/notices/USN-6131-1 8. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5917-1 advisory. https://ubuntu.com/security/notices/USN-5917-1 9. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 10. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability

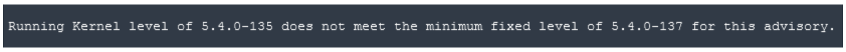
	as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 11. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory. https://ubuntu.com/security/notices/USN-6027-1 12. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory. https://ubuntu.com/security/notices/USN-6094-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`
Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-146 for this advisory.`
Recommendation	Update the affected kernel package

192.168.40.6 – file server 2

Host Information

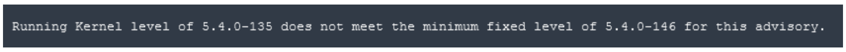
IP: 192.168.40.6
OS: Ubuntu 20.04

Finding

Severity	**Critical**
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5804-1) 2. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5813-1)
Description	1. The remote Ubuntu 16.04 ESM / 18.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5804-1 advisory. https://ubuntu.com/security/notices/USN-5804-1 2. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5813-1 advisory. https://ubuntu.com/security/notices/USN-5813-1
CVSS Score	10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`
Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-137 for this advisory.`
Recommendation	Update the affected kernel package

Severity	**High**
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 20.04 LTS : Linux kernel vulnerabilities (USN-5980-1) 2. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5853-1) 3. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5874-1) 4. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-5791-1) 5. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1) 6. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) 7. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) 8. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities

	(USN-5917-1) 9. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 10. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1) 11. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)
Description	1. The remote Ubuntu 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5980-1 advisory. https://ubuntu.com/security/notices/USN-5980-1 2. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5853-1 advisory. https://ubuntu.com/security/notices/USN-5853-1 3. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5874-1 advisory. https://ubuntu.com/security/notices/USN-5874-1 4. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5791-1 advisory. https://ubuntu.com/security/notices/USN-5791-1 5. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6047-1 advisory. https://ubuntu.com/security/notices/USN-6047-1 6. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 7. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory. https://ubuntu.com/security/notices/USN-6131-1 8. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-5917-1 advisory. https://ubuntu.com/security/notices/USN-5917-1 9. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 10. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory. https://ubuntu.com/security/notices/USN-6027-1

	11. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory. https://ubuntu.com/security/notices/USN-6094-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-135`
Evidence	 `Running Kernel level of 5.4.0-135 does not meet the minimum fixed level of 5.4.0-146 for this advisory.`
Recommendation	Update the affected kernel package

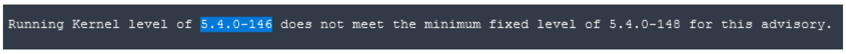
192.168.30.2 – tenant server 1a

Host Information

IP:	192.168.30.2
OS:	Ubuntu 20.04

Finding

Severity	High
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1) 2. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) 3. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) 4. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 5. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1) 6. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)
Description	1. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6047-1 advisory. https://ubuntu.com/security/notices/USN-6047-1 2. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 3. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory. https://ubuntu.com/security/notices/USN-6131-1 4. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 5. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory https://ubuntu.com/security/notices/USN-6027-1 6. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory. https://ubuntu.com/security/notices/USN-6094-1

CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-146`
Evidence	 `Running Kernel level of 5.4.0-146 does not meet the minimum fixed level of 5.4.0-148 for this advisory.`
Recommendation	Update the affected kernel package

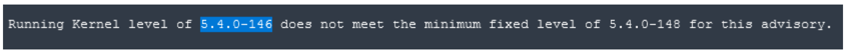
192.168.30.3 – tenant server 1b

Host Information

IP:	192.168.30.3
OS:	Ubuntu 20.04

Finding

Severity	**High**
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : Linux kernel vulnerability (USN-6047-1) 2. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) 3. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) 4. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 5. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6027-1) 6. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)
Description	1. The remote Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS host has a package installed that is affected by a vulnerability as referenced in the USN-6047-1 advisory. https://ubuntu.com/security/notices/USN-6047-1 2. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 3. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory. https://ubuntu.com/security/notices/USN-6131-1 4. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 5. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6027-1 advisory https://ubuntu.com/security/notices/USN-6027-1 6. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory. https://ubuntu.com/security/notices/USN-6094-1

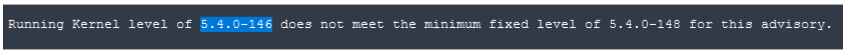
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-146`
Evidence	 `Running Kernel level of 5.4.0-146 does not meet the minimum fixed level of 5.4.0-148 for this advisory.`
Recommendation	Update the affected kernel package

192.168.30.4 – tenant server 2a

Host Information

IP: 192.168.30.4
OS: Ubuntu 20.04

Finding

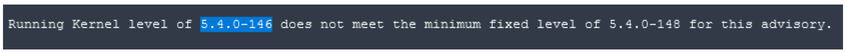
Severity	High
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) 2. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6131-1) 3. Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 : Linux kernel vulnerabilities (USN-6193-1) 4. Ubuntu 18.04 LTS / 20.04 LTS : Linux kernel vulnerabilities (USN-6094-1)
Description	1. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 2. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6131-1 advisory. https://ubuntu.com/security/notices/USN-6131-1 3. The remote Ubuntu 18.04 ESM / 20.04 LTS / 22.04 LTS / 23.04 host has a package installed that is affected by a vulnerability as referenced in the USN-6193-1 advisory. https://ubuntu.com/security/notices/USN-6193-1 4. The remote Ubuntu 18.04 LTS / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6094-1 advisory. https://ubuntu.com/security/notices/USN-6094-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-148`
Evidence	 `Running Kernel level of 5.4.0-146 does not meet the minimum fixed level of 5.4.0-148 for this advisory.`
Recommendation	Update the affected kernel package

192.168.30.5 – tenant server 2b

Host Information

IP:	192.168.30.5
OS:	Ubuntu 20.04

Finding

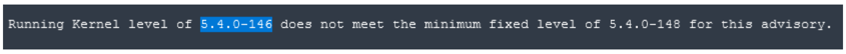
Severity	High
Name	Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1)
Description	The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-153`
Evidence	 `Running Kernel level of 5.4.0-146 does not meet the minimum fixed level of 5.4.0-148 for this advisory.`
Recommendation	Update the affected kernel package

192.168.30.6 – tenant server 3

Host Information

IP:	192.168.30.6
OS:	Ubuntu 20.04

Finding

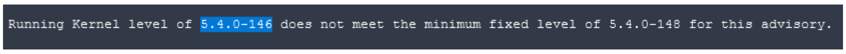
Severity	**High**
Name	Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1)
Description	The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	`5.4.0-153`
Evidence	 `Running Kernel level of 5.4.0-146 does not meet the minimum fixed level of 5.4.0-148 for this advisory.`
Recommendation	Update the affected kernel package

192.168.30.7 – tenant server 4

Host Information

IP:	192.168.30.7
OS:	Ubuntu 20.04

Finding

Severity	High
Name	Multiple Vulnerability on Kernel used 1. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6251-1) 2. Ubuntu 18.04 ESM / 20.04 LTS : Linux kernel vulnerabilities (USN-6284-1)
Description	1. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6251-1 advisory. https://ubuntu.com/security/notices/USN-6251-1 2. The remote Ubuntu 18.04 ESM / 20.04 LTS host has a package installed that is affected by multiple vulnerabilities as referenced in the USN-6284-1 advisory. https://ubuntu.com/security/notices/USN-6284-1
CVSS Score	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
Affected kernel	5.4.0-148
Evidence	 Running Kernel level of 5.4.0-146 does not meet the minimum fixed level of 5.4.0-148 for this advisory.
Recommendation	Update the affected kernel package

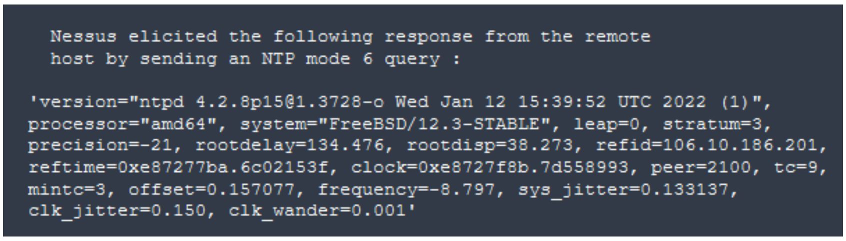
220.100.160.241 – pfsense 2

Host Information

IP:	220.100.160.241
OS:	Ubuntu 20.04

Finding

Severity	**Medium**
Name	Network Time Protocol (NTP) Mode 6 Scanner
Description	The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition. https://ntpscan.shadowserver.org
CVSS Score	5.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L)
Affected Port	123/udp/ntp

Evidence	
	Nessus elicited the following response from the remote
	host by sending an NTP mode 6 query :
	
	'version="ntpd 4.2.8p15@1.3728-o Wed Jan 12 15:39:52 UTC 2022 (1)",
	processor="amd64", system="FreeBSD/12.3-STABLE", leap=0, stratum=3,
	precision=-21, rootdelay=134.476, rootdisp=38.273, refid=106.10.186.201,
	reftime=0xe87277ba.6c02153f, clock=0xe8727f8b.7d558993, peer=2100, tc=9,
	mintc=3, offset=0.157077, frequency=-8.797, sys_jitter=0.133137,
	clk_jitter=0.150, clk_wander=0.001'

Recommendation	Restrict NTP mode 6 queries.

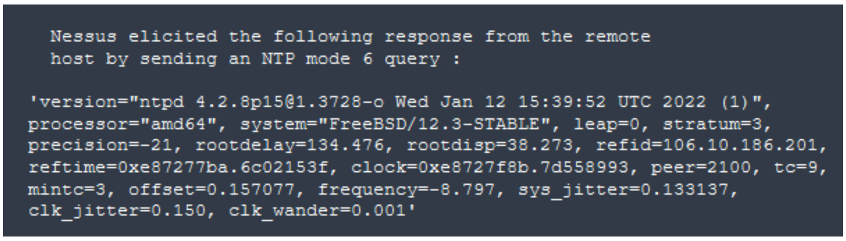
220.100.160.242 – pfsense 1

Host Information

IP:	220.100.160.242
OS:	Ubuntu 20.04

Finding

Severity	**Medium**
Name	Network Time Protocol (NTP) Mode 6 Scanner
Description	The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition. https://ntpscan.shadowserver.org
CVSS Score	5.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L)
Affected Port	123/udp/ntp

Evidence	
	Nessus elicited the following response from the remote
	host by sending an NTP mode 6 query :
	
	'version="ntpd 4.2.8p15@1.3728-o Wed Jan 12 15:39:52 UTC 2022 (1)",
	processor="amd64", system="FreeBSD/12.3-STABLE", leap=0, stratum=3,
	precision=-21, rootdelay=134.476, rootdisp=38.273, refid=106.10.186.201,
	reftime=0xe87277ba.6c02153f, clock=0xe8727f8b.7d558993, peer=2100, tc=9,
	mintc=3, offset=0.157077, frequency=-8.797, sys_jitter=0.133137,
	clk_jitter=0.150, clk_wander=0.001'

Recommendation	Restrict NTP mode 6 queries.