

Vulnerability Management

Masterschool

Network Vulnerability Assessment Scan Report for ABC Organization

Nessus Basic Network Scan

By **Babatunde Ojo**

Masterschool TryHackMe Room:

<https://tryhackme.com/room/masterschoolvulnerability>

July 13, 2023

Instructor: Mr James Key

Table of Contents

Scope of Engagement.....3

Scoring Methodology.....4

Vital Statistics.....5

Executive Summary.....6

Vulnerabilities.....7

Critical Vulnerability.....7

 CVSSv3.0 Base Score: 10.0.....7

 CVSSv3.0 Base Score: 9.8.....8

High Vulnerability.....26

 CVSSv3.0 Base score: 8.8 - 7.0.....26

Medium Vulnerabilities.....28

 CVSSv3.0 Base score: 6.8 - 4.0.....28

Remediation.....30

Conclusion.....31

References.....32

Scope of Engagement

This vulnerability assessment report provides an overview of the basic network scan conducted for ABC Organization. The purpose of this assessment is to identify potential web vulnerabilities across all ports within the organization's network infrastructure. By performing a comprehensive scan, we aim to evaluate the security posture of ABC Organization's web-based assets and provide actionable insights to enhance their overall cybersecurity resilience. The basic network scan focuses on detecting vulnerabilities that may expose web applications or services to potential exploits, thereby aiding ABC Organization in proactively addressing these weaknesses and minimizing the risk of unauthorized access or data breaches. This report will outline the findings, highlight critical vulnerabilities, and offer recommendations to strengthen ABC Organization's web security infrastructure.

Scoring Methodology

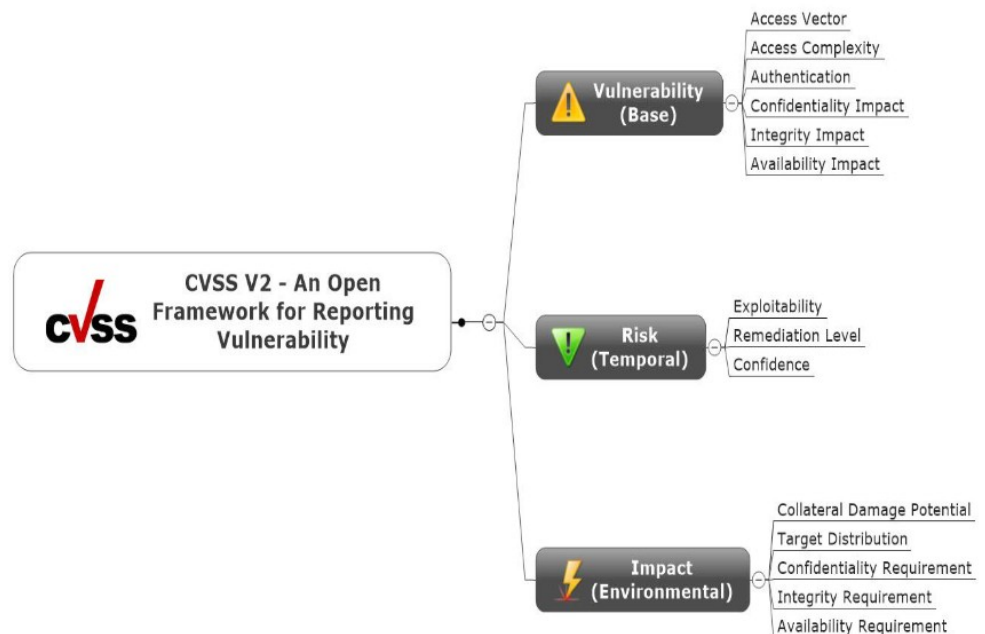
Nessus uses CVSS scores and dynamic Tenable-calculated Vulnerability Priority Rating (VPR) to quantify the risk and urgency of a vulnerability.

Tenable Nessus assigns all vulnerabilities a severity (**Info, Low, Medium, High, or Critical**) based on the vulnerability's static CVSSv2 or CVSSv3 score.

Severity	CVSSv2 Range	CVSSv3 Range
Critical	The plugin's highest vulnerability CVSSv2 score is 10.0.	The plugin's highest vulnerability CVSSv3 score is between 9.0 and 10.0.
High	The plugin's highest vulnerability CVSSv2 score is between 7.0 and 9.9.	The plugin's highest vulnerability CVSSv3 score is between 7.0 and 8.9.
Medium	The plugin's highest vulnerability CVSSv2 score is between 4.0 and 6.9.	The plugin's highest vulnerability CVSSv3 score is between 4.0 and 6.9.
Low	The plugin's highest vulnerability CVSSv2 score is between 0.1 and 3.9.	The plugin's highest vulnerability CVSSv3 score is between 0.1 and 3.9.
Info	The plugin's highest vulnerability CVSSv2 score is 0.	The plugin's highest vulnerability CVSSv3 score is 0.

CVSSv2 and CVSSv3 uses three metrics groups: Base, Temporal and Environmental

CVSSv3 aims to improve the user experience by providing clearer and more concise scoring guideline.



Vital Statistics

This document presents the outcomes derived from a recent comprehensive vulnerability assessment on the infrastructure of ABC organization. Serving as a concise summary of the findings, it outlines a series of actionable recommendations aimed at effectively addressing the identified events. The analysis was performed utilizing meticulously gathered data, carefully considering the following discernible characteristics:

Company Details

Company Name: ABC organization

Location: Forney, TX

Industry: Technology

Company Size: 500 Employees

Host Information

Test Start Date: 7/14/2023

DNS Name: IP-10-10-155-65.eu-west-1.compute.internal

Host IP: 10.10.115.65

Vulnerability Scanner: Tenable-Nessus

MAC: 02:EB:4E:92:AB:03

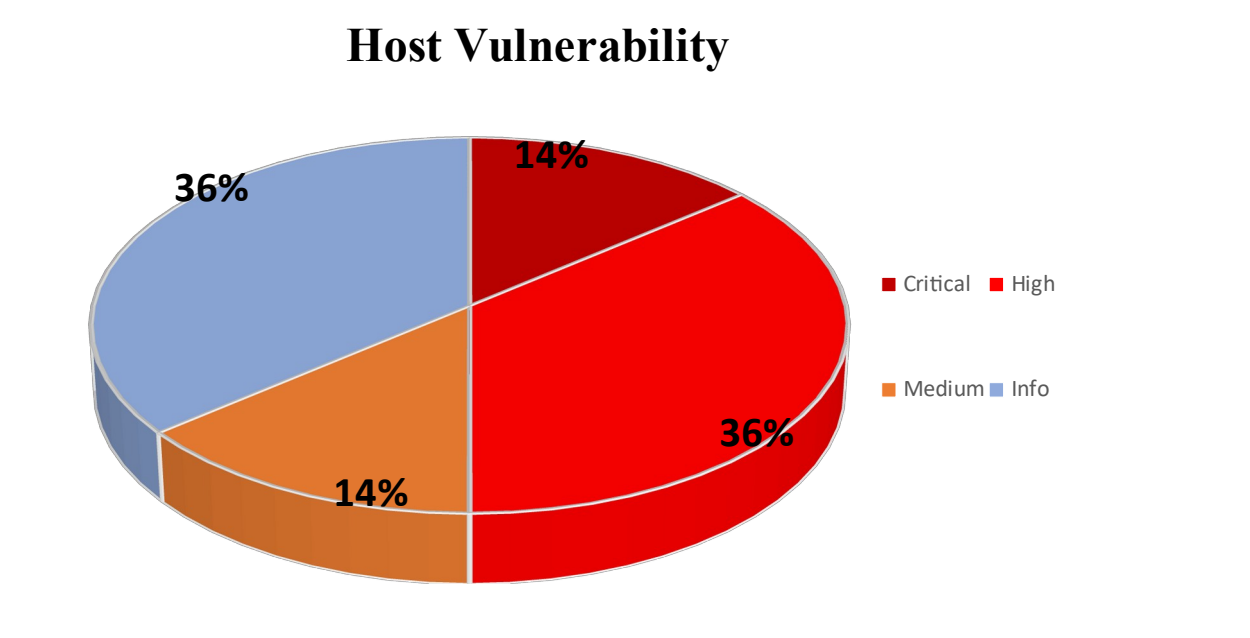
OS: Linux Kernel 4.15.0-142-generic on Ubuntu 16.04


Deployment and Methodology

A host was scanned and monitored with Tenable-Nessus. On the target system, Nessus performed a comprehensive scan with credentials, meticulously examining open ports and services on the target systems. After identifying these accessible network services, Nessus proceeds with its specialized web vulnerability detection methods to uncover potential security weaknesses in web applications and associated components. Nessus matches the identified ports and services against known vulnerabilities, then generates a detailed assessment report, presenting the findings in severity levels (CVSS scores)

Executive Summary

After a completed network scan, Nessus displays scan details using CVSSv3.0 severity base model. Below is the host 10.10.115.65 vulnerability chart based on the vulnerability score and host from Nessus.





Report generated by Nessus™

ABC Organization with credentials

Fri, 14 Jul 2023 22:36:14 EDT

TABLE OF CONTENTS

Vulnerabilities by Host

• 10.10.155.65

Vulnerabilities by Host

Collapse All | Expand All

10.10.155.65

39

CRITICAL

100

HIGH

40

MEDIUM

0

LOW

100

INFO

Vulnerabilities

Critical Vulnerability

CVSSv3.0 Base Score: 10.0

33850 - Unix Operating System Unsupported Version Detection -

Unix Operating system on Extended Support (cvss: 10)

Description:

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Evidence:

Ubuntu 16.04 support ended on 2021-04-30 (end of maintenance) / 2026-04-30 (end of extended security maintenance).
Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : <https://wiki.ubuntu.com/Releases>

Solution:

Upgrade to a version of the Unix operating system that is currently supported to ensure continuous security updates.

CVSSv3.0 Base Score: 9.8

159882 - Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS : klibc vulnerabilities (USN-5379-1) -

Klibc installed package version has integer overflow vulnerabilities

Description:

The remote Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 20.04 LTS host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5379-1 advisory. An attacker could possibly use this issue to cause a crash, resulting in a denial of service, or possibly execute arbitrary code.

Evidence:

```
- Installed package : klibc-utils_2.0.4-8ubuntu1.16.04.4
Fixed package : klibc-utils_2.0.4-8ubuntu1.16.04.4+esm1

- Installed package : libklibc_2.0.4-8ubuntu1.16.04.4
Fixed package : libklibc_2.0.4-8ubuntu1.16.04.4+esm1
```

Solution:

Update the affected klibc-utils, libklibc and / or libklibc-dev packages.

163104 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS / 21.10 / 22.04 LTS : Python vulnerability (USN-5519-1)

Python incorrectly handled certain inputs

Description:

In Python (aka CPython) through 3.10.4, the mailcap module does not add escape characters into commands discovered in the system mailcap file. This may allow attackers to inject shell commands into applications that call mailcap.findmatch with untrusted input.

Evidence:

```
- Installed package : libpython2.7_2.7.12-1ubuntu0~16.04.18
Fixed package : libpython2.7_2.7.12-1ubuntu0~16.04.18+esm2

- Installed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18
Fixed package : libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm2

- Installed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18
Fixed package : libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18+esm2

- Installed package : libpython3.5_3.5.2-2ubuntu0~16.04.13
Fixed package : libpython3.5_3.5.2-2ubuntu0~16.04.13+esm3

- Installed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13
Fixed package : libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm3

- Installed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13
Fixed package : libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13+esm3

- Installed package : python2.7_2.7.12-1ubuntu0~16.04.18
Fixed package : python2.7_2.7.12-1ubuntu0~16.04.18+esm2

- Installed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18
Fixed package : python2.7-minimal_2.7.12-1ubuntu0~16.04.18+esm2

- Installed package : python3.5_3.5.2-2ubuntu0~16.04.13
Fixed package : python3.5_3.5.2-2ubuntu0~16.04.13+esm3

- Installed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13
Fixed package : python3.5-minimal_3.5.2-2ubuntu0~16.04.13+esm3
```

Solution:

Update the affected packages: libpython2.7_2.7.12-1ubuntu0~16.04.18 | libpython2.7-minimal_2.7.12-1ubuntu0~16.04.18 | libpython2.7-stdlib_2.7.12-1ubuntu0~16.04.18 | libpython3.5_3.5.2-2ubuntu0~16.04.13 | libpython3.5-minimal_3.5.2-2ubuntu0~16.04.13 | libpython3.5-stdlib_3.5.2-2ubuntu0~16.04.13 | python2.7_2.7.12-1ubuntu0~16.04.18 | python2.7-minimal_2.7.12-1ubuntu0~16.04.18 | python3.5_3.5.2-2ubuntu0~16.04.13 | python3.5-minimal_3.5.2-2ubuntu0~16.04.13

164287 - Ubuntu 16.04 ESM / 18.04 LTS / 20.04 LTS : rsync vulnerability (USN-5573-1) -

zlib version incorrectly handled memory when performing certain inflate operations

Description:

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-5573-1 advisory. zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field.

Evidence:

```
- Installed package : rsync_3.1.1-3ubuntu1.3  
Fixed package : rsync_3.1.1-3ubuntu1.3+esm2
```

Solution:

Update the affected rsync package: rsync_3.1.1-3ubuntu1.3

162515 - Ubuntu 16.04 ESM / 18.04 LTS : Apache HTTP Server regression (USN-5487-3)

USN-5487-2 reverted the patches that caused the regression in Ubuntu 14.04 ESM

Description:

Apache HTTP Server mod_proxy_ajp incorrectly handled certain crafted request. A remote attacker could possibly use this issue to perform an HTTP Request Smuggling attack. The following common vulnerabilities and Exposures are included: (CVE-2022-26377) (CVE-2022-28615) (CVE-2022-28614) (CVE-2022-29404) (CVE-2022-30522) (CVE-2022-30556)

Evidence:

```
- Installed package : apache2_2.4.18-2ubuntu3.17
Fixed package : apache2_2.4.18-2ubuntu3.17+esm7

- Installed package : apache2-bin_2.4.18-2ubuntu3.17
Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm7

- Installed package : apache2-data_2.4.18-2ubuntu3.17
Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm7

- Installed package : apache2-utils_2.4.18-2ubuntu3.17
Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm7
```

Solution:

Update the affected packages: apache2_2.4.18-2ubuntu3.17 | apache2-bin_2.4.18-2ubuntu3.17 | apache2-data_2.4.18-2ubuntu3.17 | apache2-utils_2.4.18-2ubuntu3.17

164275 - Ubuntu 16.04 ESM / 18.04 LTS : zlib vulnerability (USN-5570-1)

-

Buffer overflow on zlib package version installed

Description: The remote Ubuntu 16.04 ESM / 18.04 LTS host has packages installed that are affected by a vulnerability as referenced in the USN-5570-1 advisory. zlib through 1.2.12 has a heap-based buffer over-read or buffer overflow in inflate in inflate.c via a large gzip header extra field.

Evidence:

```
- Installed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3  
Fixed package : zlib1g_1:1.2.8.dfsg-2ubuntu4.3+esm2
```

Solution:

Update the affected package: `zlib1g_1:1.2.8.dfsg-2ubuntu4.3`

161386 - Ubuntu 16.04 ESM : OpenLDAP vulnerability (USN-5424-2)

OpenLDAP incorrectly handled certain SQL statements within LDAP queries

Description:

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5424-2 advisory. In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection vulnerability exists in the experimental back-sql backend to slapd, via a SQL statement within an LDAP query. This can occur during an LDAP search operation when the search filter is processed, due to a lack of proper escaping. (CVE-2022-29155)

Evidence:

```
- Installed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.13
Fixed package : libldap-2.4-2_2.4.42+dfsg-2ubuntu3.13+esm1
```

Solution:

Update the affected package: libldap-2.4-2_2.4.42+dfsg-2ubuntu3.13

161611 - Ubuntu 16.04 ESM : OpenSSL vulnerabilities (USN-5402-2)

OpenSSL incorrectly handled the c_rehash script

Description:

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5402-2 advisory. The c_rehash script does not properly sanitize shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed.

Evidence:

```
- Installed package : libssl1.0.0_1.0.2g-1ubuntu4.20  
Fixed package : libssl1.0.0_1.0.2g-1ubuntu4.20+esm3  
  
- Installed package : openssl_1.0.2g-1ubuntu4.20  
Fixed package : openssl_1.0.2g-1ubuntu4.20+esm3
```

Solution:

Update the affected libssl-dev, libssl1.0.0 and / or openssl packages: libssl1.0.0_1.0.2g-1ubuntu4.20 | openssl_1.0.2g-1ubuntu4.20

161449 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5433-1)

-

163107 - Ubuntu 16.04 ESM : Vim vulnerabilities (USN-5516-1)

-

162514 - Ubuntu 16.04 ESM : Vim vulnerability (USN-5492-1)

-

Vim incorrectly handled memory access when opening and searching content of files

Description:

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5433-1 advisory, USN-5516-1 advisory and USN-5492-1 advisory. vim is vulnerable to Heap-based Buffer Overflow (CVE-2021-3973, CVE-2021-3984, CVE-2021-4019), vim is vulnerable to Use After Free (CVE-2021-3974, CVE-2021-4069, CVE-2021-4192), Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2. (CVE-2022-0261), Heap-based Buffer Overflow in vim/vim prior to 8.2. (CVE-2022-0318), Use after free in utf_ptr2char in GitHub repository vim/vim prior to 8.2.4646. (CVE-2022-1154).

Vim is vulnerable to Out-of-bounds Write in GitHub repository vim/vim prior to 8.2. (CVE-2022-2000, CVE-2022-2210), Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2. (CVE-2022-2207), Use After Free in GitHub repository vim/vim prior to 8.2. (CVE-2022-2042).

Evidence:

```
- Installed package : vim-common_2:7.4.1689-3ubuntu1.5
Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm4

- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.5
Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm4

- Installed package : vim-common_2:7.4.1689-3ubuntu1.5
Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm11

- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.5
Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm11

- Installed package : vim-common_2:7.4.1689-3ubuntu1.5
Fixed package : vim-common_2:7.4.1689-3ubuntu1.5+esm7

- Installed package : vim-tiny_2:7.4.1689-3ubuntu1.5
Fixed package : vim-tiny_2:7.4.1689-3ubuntu1.5+esm7
```

Solution:

Update the affected package: vim-common_2:7.4.1689-3ubuntu1.5

161690 - Ubuntu 16.04 ESM : dpkg vulnerability (USN-5446-2)

A malicious source package could write files outside the unpack directory.

Description:

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5446-2 advisory. Dpkg::Source::Archive in dpkg, the Debian package management system, before version 1.21.8, 1.20.10, 1.19.8, 1.18.26 is prone to a directory traversal vulnerability. When extracting untrusted source packages in v2 and v3 source package formats that include a debian.tar, the in-place extraction can lead to directory traversal situations on specially crafted orig.tar and debian.tar tarballs. (CVE-2022-1664)

Evidence:

```
- Installed package : dpkg_1.18.4ubuntu1.6
Fixed package : dpkg_1.18.4ubuntu1.7+esm1

- Installed package : dpkg-dev_1.18.4ubuntu1.6
Fixed package : dpkg-dev_1.18.4ubuntu1.7+esm1

- Installed package : libdpkg-perl_1.18.4ubuntu1.6
Fixed package : libdpkg-perl_1.18.4ubuntu1.7+esm1
```

Solution:

Update the affected packages: dpkg_1.18.4ubuntu1.6 | dpkg-dev_1.18.4ubuntu1.6 | libdpkg-perl_1.18.4ubuntu1.6

161452 - Ubuntu 16.04 ESM : libXfixes vulnerability (USN-5437-1)

libXfixes could be made to crash or run programs if it received specially crafted input.

Description:

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5437-1 advisory. Integer overflow in X.org libXfixes before 5.0.3 on 32-bit platforms might allow remote X servers to gain privileges via a length value of INT_MAX, which triggers the client to stop reading data and get out of sync. (CVE-2016-7944)

Evidence:

```
- Installed package : libxfixes3_1:5.0.1-2  
Fixed package : libxfixes3_1:5.0.1-2ubuntu0.1~esm1
```

Solution:

Update the affected libxfixes3 packages: libxfixes3_1:5.0.1-2

161450 - Ubuntu 16.04 ESM : libXrender vulnerabilities (USN-5436-1)

libXrender incorrectly handled certain responses.

Description:

The remote Ubuntu 16.04 ESM host has packages installed that are affected by multiple vulnerabilities as referenced in the USN-5436-1 advisory. Multiple buffer overflows in the (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXrender before 0.9.10 allow remote X servers to trigger out-of-bounds write operations via vectors involving length fields. (CVE-2016-7949)

The XRenderQueryFilters function in X.org libXrender before 0.9.10 allows remote X servers to trigger out-of-bounds write operations via vectors involving filter name lengths. (CVE-2016-7950)

Solution:

Update the affected libxrender1 package: libxrender1_1:0.9.9-0ubuntu1

161630 - Ubuntu 16.04 ESM : libXv vulnerability (USN-5449-1)

libXv could be made to crash or run programs if it received specially crafted input.

Description:

The remote Ubuntu 16.04 ESM host has packages installed that are affected by a vulnerability as referenced in the USN-5449-1 advisory. The (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXv before 1.0.11 allow remote X servers to trigger out-of-bounds memory access operations via vectors involving length specifications in received data. (CVE-2016-5407)

Evidence:

```
- Installed package : libxv1_2:1.0.10-1  
Fixed package : libxv1_2:1.0.10-1ubuntu0.16.04.1~esm1
```

Solution:

Update the affected libxv1 packages

161634 - Ubuntu 16.04 ESM : ncurses vulnerabilities (USN-5448-1)

-

ncurses - shared libraries for terminal handling

Description:

ncurses was not properly checking array bounds when executing the `fmt_entry` function, which could result in an out-of-bounds write. An attacker could possibly use this issue to execute arbitrary code. (CVE-2017-10684)

ncurses was incorrectly handling loops in `libtic`, which could lead to the execution of an infinite loop. An attacker could possibly use this issue to cause a denial of service. (CVE-2017-13728)

Evidence:

```
- Installed package : libncurses5_6.0+20160213-1ubuntu1
Fixed package : libncurses5_6.0+20160213-1ubuntu1+esm1

- Installed package : libncursesw5_6.0+20160213-1ubuntu1
Fixed package : libncursesw5_6.0+20160213-1ubuntu1+esm1

- Installed package : libtinfo5_6.0+20160213-1ubuntu1
Fixed package : libtinfo5_6.0+20160213-1ubuntu1+esm1

- Installed package : ncurses-base_6.0+20160213-1ubuntu1
Fixed package : ncurses-base_6.0+20160213-1ubuntu1+esm1

- Installed package : ncurses-bin_6.0+20160213-1ubuntu1
Fixed package : ncurses-bin_6.0+20160213-1ubuntu1+esm1

- Installed package : ncurses-term_6.0+20160213-1ubuntu1
Fixed package : ncurses-term_6.0+20160213-1ubuntu1+esm1
```

Solution:

Update the affected packages: `libncurses5_6.0+20160213-1ubuntu1` | `libncursesw5_6.0+20160213-1ubuntu1` | `libtinfo5_6.0+20160213-1ubuntu1` | `ncurses-base_6.0+20160213-1ubuntu1` | `ncurses-term_6.0+20160213-1ubuntu1`

158212 - Ubuntu 16.04 LTS / 18.04 LTS / 20.04 LTS / 21.10 : Expat vulnerabilities (USN-5288-1) -

Expat incorrectly handled certain files.

Description:

Expat incorrectly handled certain files. An attacker could possibly use this issue to cause a crash or execute arbitrary code. Contains various CVEs in relation to integer overflow - (CVE-2021-46143), (CVE-2022-22822), (CVE-2022-22823), (CVE-2022-22824), (CVE-2022-22825), (CVE-2022-22826), (CVE-2022-22827), (CVE-2022-23852), (CVE-2022-23990)

Evidence:

```
- Installed package : libexpat1_2.1.0-7ubuntu0.16.04.5  
Fixed package : libexpat1_2.1.0-7ubuntu0.16.04.5+esm2
```

Solution:

Update the affected package: libexpat1_2.1.0-7ubuntu0.16.04.5

157160 - Ubuntu 16.04 LTS / 18.04 LTS : shadow vulnerabilities (USN-5254-1)

shadow incorrectly handled certain inputs.

Description:

In shadow before 4.5, the new users' tool could be made to manipulate internal data structures in ways unintended by the authors. Malformed input may lead to crashes (with a buffer overflow or other memory corruption) or other unspecified behaviors. This crosses a privilege boundary in, for example, certain web-hosting environments in which a Control Panel allows an unprivileged user account to create subaccounts. (CVE-2017-12424)

An issue was discovered in shadow 4.5. newgidmap (in shadow-utils) is setuid and allows an unprivileged user to be placed in a user namespace where setgroups(2) is permitted. This allows an attacker to remove themselves from a supplementary group, which may allow access to certain filesystem paths if the administrator has used group blacklisting (e.g., chmod g-rwx) to restrict access to paths. This flaw effectively reverts a security feature in the kernel (in particular, the /proc/self/setgroups knob) to prevent this sort of privilege escalation. (CVE-2018-7169)

Evidence:

```
- Installed package : login_1:4.2-3.1ubuntu5.4
Fixed package : login_1:4.2-3.1ubuntu5.5+esm1

- Installed package : passwd_1:4.2-3.1ubuntu5.4
Fixed package : passwd_1:4.2-3.1ubuntu5.5+esm1
```

Solution:

Update the affected login, and passwd packages: login_1:4.2-3.1ubuntu5.4 |
passwd_1:4.2-3.1ubuntu5.4

150942 - Ubuntu 16.04 LTS : Apache HTTP Server vulnerabilities (USN-4994-2)

-

153766 - Ubuntu 16.04 LTS : Apache HTTP Server vulnerabilities (USN-5090-2)

-

156568 - Ubuntu 16.04 LTS : Apache HTTP Server vulnerabilities (USN-5212-2)

-

159058 - Ubuntu 16.04 LTS : Apache HTTP Server vulnerabilities (USN-5333-2)

-

Apache HTTP Server incorrectly handled various security settings

Description:

Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow (CVE-2020-35452)

Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service (CVE-2021-26690)

Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier. (CVE-2021-34798)

Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling (CVE-2022-22720)

Evidence:

```
- Installed package : apache2_2.4.18-2ubuntu3.17
Fixed package : apache2_2.4.18-2ubuntu3.17+esm1

- Installed package : apache2-bin_2.4.18-2ubuntu3.17
Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm1

- Installed package : apache2-data_2.4.18-2ubuntu3.17
Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm1

- Installed package : apache2-utils_2.4.18-2ubuntu3.17
Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm1
```

```
- Installed package : apache2_2.4.18-2ubuntu3.17
Fixed package : apache2_2.4.18-2ubuntu3.17+esm2

- Installed package : apache2-bin_2.4.18-2ubuntu3.17
Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm2

- Installed package : apache2-data_2.4.18-2ubuntu3.17
Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm2

- Installed package : apache2-utils_2.4.18-2ubuntu3.17
Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm2

- Installed package : apache2_2.4.18-2ubuntu3.17
Fixed package : apache2_2.4.18-2ubuntu3.17+esm4

- Installed package : apache2-bin_2.4.18-2ubuntu3.17
Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm4

- Installed package : apache2-data_2.4.18-2ubuntu3.17
Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm4

- Installed package : apache2-utils_2.4.18-2ubuntu3.17
Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm4

- Installed package : apache2_2.4.18-2ubuntu3.17
Fixed package : apache2_2.4.18-2ubuntu3.17+esm5

- Installed package : apache2-bin_2.4.18-2ubuntu3.17
Fixed package : apache2-bin_2.4.18-2ubuntu3.17+esm5

- Installed package : apache2-data_2.4.18-2ubuntu3.17
Fixed package : apache2-data_2.4.18-2ubuntu3.17+esm5

- Installed package : apache2-utils_2.4.18-2ubuntu3.17
Fixed package : apache2-utils_2.4.18-2ubuntu3.17+esm5
```

Solution:

Update the affected packages: apache2_2.4.18-2ubuntu3.17 | apache2-bin_2.4.18-2ubuntu3.17 | apache2-data_2.4.18-2ubuntu3.17 | apache2-utils_2.4.18-2ubuntu3.17 | apache2_2.4.18-2ubuntu3.17

158680 - Ubuntu 16.04 LTS : GNU C Library vulnerabilities (USN-5310-2)

-

151919 - Ubuntu 16.04 LTS : GNU binutils vulnerabilities (USN-4336-2)

-

GNU C library getcwd function incorrectly handled buffers.

Description:

GNU binutils contained a large number of security issues. If a user or automated system were tricked into processing a specially-crafted file, a remote attacker could cause GNU binutils to crash, resulting in a denial of service, or possibly execute arbitrary code.

These vulnerabilities have over 60 CVEs associated to it!

Evidence:

```
- Installed package : binutils_2.26.1-1ubuntu1~16.04.8
Fixed package : binutils_2.26.1-1ubuntu1~16.04.8+esm1
```

```
- Installed package : libc-bin_2.23-0ubuntu11.3
Fixed package : libc-bin_2.23-0ubuntu11.3+esm1
```

```
- Installed package : libc-dev-bin_2.23-0ubuntu11.3
Fixed package : libc-dev-bin_2.23-0ubuntu11.3+esm1
```

```
- Installed package : libc6_2.23-0ubuntu11.3
Fixed package : libc6_2.23-0ubuntu11.3+esm1
```

```
- Installed package : libc6-dev_2.23-0ubuntu11.3
Fixed package : libc6-dev_2.23-0ubuntu11.3+esm1
```

```
- Installed package : locales_2.23-0ubuntu11.3
Fixed package : locales_2.23-0ubuntu11.3+esm1
```

```
- Installed package : multiarch-support_2.23-0ubuntu11.3
Fixed package : multiarch-support_2.23-0ubuntu11.3+esm1
```

Solution:

Update the affected packages: libc-bin_2.23-0ubuntu11.3 | libc-dev-bin_2.23-0ubuntu11.3 | libc6_2.23-0ubuntu11.3 | libc6-dev_2.23-0ubuntu11.3 | locales_2.23-0ubuntu11.3 | multiarch-support_2.23-0ubuntu11.3 | binutils_2.26.1-1ubuntu1~16.04.8

High Vulnerability

CVSSv3.0 Base score: 8.8 - 7.0

Vulnerability	Count
Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS : Linux kernel vulnerabilities	19
Ubuntu 16.04 ESM : Vim vulnerabilities	6
Ubuntu 16.04 LTS : OpenSSL vulnerability	3
Ubuntu 16.04 LTS : DHCP vulnerability	1
Ubuntu 16.04 ESM : Python vulnerability	4
Ubuntu 16.04 LTS : curl vulnerabilities	2
Ubuntu 16.04 LTS : tcpdump vulnerabilities	1

DOS, TLS certificate, DHCP v4, Python info disclosure, Curl, tcpdump

The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial-of-service attack.

any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self- signed certificate to trigger the loop during verification of the certificate signature.

In ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16, ISC DHCP 4.4.0 -> 4.4.2 (Other branches of ISC DHCP (i.e., releases in the 4.0.x series or lower and releases in the 4.3.x series) are beyond their End-of-Life (EOL) and no longer supported by ISC. If the dhcpd server binary was built for a 32-bit architecture AND the -fstack-protection-strong flag was specified to the compiler, dhcpd may exit while parsing a lease file containing an objectionable lease, resulting in lack of service to clients.

Python 3.x through 3.10 has an open redirection vulnerability in lib/http/server.py due to no protection against multiple (/) at the beginning of URI path which may leads to information disclosure.

Http server is not recommended for production. It only implements basic security checks.

A user can tell curl $\geq 7.20.0$ and $\leq 7.78.0$ to require a successful upgrade to TLS when speaking to an IMAP, POP3 or FTP server. This requirement could be bypassed if the server would return a properly crafted but perfectly legitimate response. This flaw would then make curl silently continue its operations exposing possibly sensitive data in clear text over the network

The command-line argument parser in tcpdump before 4.99.0 has a buffer overflow in tcpdump.c:read_infile(). To trigger this vulnerability the attacker needs to create a 4GB file on the local filesystem and to specify the file name as the value of the -F command-line argument of tcpdump.

Medium Vulnerabilities

CVSSv3.0 Base score: 6.8 - 4.0

Vulnerability	Count
SSL certificate cannot be Trusted	1
Cron regression	2
curl vulnerabilities	2
HTTP-Daemon vulnerability	1
systemd vulnerabilities	1

SSL, Cron, Curl, HTTP, Systemd vulnerabilities

SSL certificates play a crucial role in the operation of web server serving two primary purposes Firstly, they facilitate the establishment of a secure communication channel for the transmission of data between web browsers and servers. It is imperative to ensure that the encryption utilized during this data exchange remains robust and resilient, as any compromise in its strength can potentially expose sensitive information. In such a scenario, determined attackers with significant resources at their disposal may exploit vulnerabilities in the encryption methods to decrypt and gain unauthorized access to previously encrypted data stored on the web server.

The certificate chain contains a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.

the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified.

In the cron package through 3.0p11-128 on Debian, and through 3.0p11-128ubuntu2 on Ubuntu, the postinst maintainer script allows for group-crontab-to-root privilege escalation via symlink attacks against unsafe usage of the chown and chmod programs.

When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly.

This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client.

HTTP Daemon is a simple http server class written in perl. Versions prior to 6.15 are subject to a vulnerability which could potentially be exploited to gain privileged access to APIs or poison intermediate caches.

An exploitable denial-of-service vulnerability exists in Systemd 245. A specially crafted DHCP FORCERENEW packet can cause a server running the DHCP client to be vulnerable to a DHCP ACK spoofing attack. An attacker can forge a pair of FORCERENEW and DCHP ACK packets to reconfigure the server.

Remediation

- Upgrade or liquidate system running unsupported operating systems and software
 - Linux Kernel 4.15.0-142-generic on Ubuntu 16.04
 - Ubuntu 16.04 support ended on 2021-04-30 (end of maintenance) / 2026-04-30 (end of extended security maintenance). Upgrade to Ubuntu 21.04 / LTS 20.04 / LTS 18.04.
- Regular Patch management
 - Ensure proactive identification, assessment and remediation of vulnerabilities on host
 - Ensure missing patches are tested and deployed
 - Update all packages to the latest version.

Conclusion

Based on the results of the vulnerability scan conducted using Nessus on the ABC organization, comprehensive analysis reveals a significant number of vulnerabilities across various severity levels. The scan identified a total of 39 critical vulnerabilities, which require immediate attention and remediation to mitigate potential security risks. Additionally, 100 high vulnerabilities, 40 medium vulnerabilities, and 76 informational findings were detected.

These findings underscore the importance of promptly addressing the identified vulnerabilities to strengthen the organization's overall security posture. Urgent action is necessary to mitigate the critical vulnerabilities and minimize the potential for unauthorized access, data breaches, or other malicious activities.

It is recommended that the organization prioritize the remediation process, starting with the critical vulnerabilities, followed by the high and medium ones. Timely resolution of these vulnerabilities will significantly reduce the organization's attack surface and enhance its resilience against potential threats.

Furthermore, it is crucial to establish a comprehensive and ongoing vulnerability management program to proactively identify, assess, and remediate vulnerabilities within the organization's IT infrastructure. Regular vulnerability scans and timely patching of software and systems are essential measures to ensure the organization remains protected against emerging security threats.

References

Tenable Nessus Documentation: Risk Metrics Link:

<https://docs.tenable.com/nessus/Content/RiskMetrics.htm>

Tenable Nessus Plugin 164275 Link: <https://www.tenable.com/plugins/nessus/164275>

Ubuntu Security Notice USN-5570-1 Link: <https://ubuntu.com/security/notices/USN-5570-1>

Tenable Nessus Plugin 161611 Link: <https://www.tenable.com/plugins/nessus/161611>

Ubuntu Security Notice USN-5402-2 Link: <https://ubuntu.com/security/notices/USN-5402-2>

Tenable Nessus Plugin 162773 Link: <https://www.tenable.com/plugins/nessus/162773>

Ubuntu Security Notice USN-5488-2 Link: <https://ubuntu.com/security/notices/USN-5488-2>

Ubuntu Security Notice USN-5433-1 Link: <https://ubuntu.com/security/notices/USN-5433-1>

Tenable Nessus Plugin 161449 Link: <https://www.tenable.com/plugins/nessus/161449>

Tenable Nessus Plugin 163107 Link: <https://www.tenable.com/plugins/nessus/163107>

Ubuntu Security Notice USN-5516-1 Link: <https://ubuntu.com/security/notices/USN-5516-1>

Ubuntu Security Notice USN-5492-1 Link: <https://ubuntu.com/security/notices/USN-5492-1>

Tenable Nessus Plugin 162514 Link: <https://www.tenable.com/plugins/nessus/162514>

Tenable Nessus Plugin 161690 Link: <https://www.tenable.com/plugins/nessus/161690>

Ubuntu Security Notice USN-5446-2 Link: <https://ubuntu.com/security/notices/USN-5446-2>

Tenable Nessus Plugin 161452 Link: <https://www.tenable.com/plugins/nessus/161452>

Ubuntu Security Notice USN-5437-1 Link: <https://ubuntu.com/security/notices/USN-5437-1>

Tenable Nessus Plugin 161450 Link: <https://www.tenable.com/plugins/nessus/161450>

Ubuntu Security Notice USN-5436-1 Link: <https://ubuntu.com/security/notices/USN-5436-1>

Ubuntu Security Notice USN-5333-2 Link: <https://ubuntu.com/security/notices/USN-5333-2>

Tenable Nessus Plugin 159058 Link: <https://www.tenable.com/plugins/nessus/159058>

Tenable Nessus Plugin 155767 Link: <https://www.tenable.com/plugins/nessus/155767>

Ubuntu Security Notice USN-5168-3 Link: <https://ubuntu.com/security/notices/USN-5168-3>