

| Team #14 |
| --- |
|  |

# Memorandum

To: Management

From: Team #14

Date: February 18, 2023

Subject: Inventory Report

Dear [CIO Name],

We have provided an updated inventory report of all the network devices in our infrastructure, including important information such as IP addresses, current and available OS levels, and upgrade recommendations.

Attached is a table that catalogs each network device and includes the following information for each device:

* Device Name
* Device IP address
* OS Level currently installed
* Current production OS level available from the manufacturer
* Upgrade recommendation based on a vulnerability assessment of the current OS

Please take a moment to review the attached table. If you have any questions or concerns regarding the upgrade recommendations, don't hesitate to reach out.

Sincerely,

Team 14

| **Device Name** | **Device IP Address(es)** | **O/S Level Currently Installed** | **Device MAC Address** | **Current Production O/S Level** | **Upgrades Needed** | **Vulnerabilities** |
| --- | --- | --- | --- | --- | --- | --- |
| **Windows 10** | **172.31.34.5** | **Windows 10** | **00:50:56:9E:17:46** | **Windows 11** | **Upgrade to Windows 11** | **Privilege Escalation (CVE-2022-37969)**  **RCE (CVE-2022-34722)** |
| **2016 Docker/ Remote** | **Local IP: 172.20.240.10  Public IP: 172.25.20.34.97** | **Windows Server 2016 Standard** | **00:15:5D:FE:2A:A0** | **Windows Server 2022** | **Upgrade to Windows Server 2022** | **Hyper-V RCE (CVE-2021-34450)**  **Eternal Blue (CVE-2017-0144)** |
| **Debian 8.5 DNS/NTP** | **Local IP: 172.20.240.20**  **Public IP: 172.25.20.34.20** | **Debian 8.5** | **00:50:56:9E:5A:07** | **Debian 11** | **Upgrade to Debian 11** | **Privilege Escalation (CVE-2016-5696)**  **RCE (CVE-2011-1930)** |
| **Ubuntu 14 Web** | **Local IP: 172.20.242.10**  **Public IP: 172.25.20.34.23** | **Ubuntu 14.04.2** | **00:50:56:9E:94:28** | **Ubuntu 22.04** | **Upgrade to Ubuntu 22.04** | **RCE (CVE-2011-2767)**  **DOS (CVE-2014-1528)** |
| **2012 AD/DNS/ DHCP** | **Local IP: 172.20.242.200**  **Public IP: 172.25.20.34.27** | **Windows Server 2012 Standard** | **00:50:56:9E:9E:48** | **Windows Server 2022** | **Upgrade to Windows Server 2022** | **Print Spooler Privilege Escalation (CVE-2023-21760)**  **RCE (CVE-2022-44667)** |
| **Ubuntu Wkst** | **DHCP** | **Ubuntu Desktop 12.04** | **00:50:56:9E:75:D6** | **Ubuntu Desktop 22.10** | **Upgrade to Ubuntu Desktop 22.10** | **Error Handling (CVE-2020-8625)**  **Privilege Escalation (CVE-2013-2094)** |
| **Splunk** | **Local IP: 172.20.241.20**  **Public IP: 172.25.20.34.9** | **CentOS 7** | **00:50:56:9D:75:2D** | **CentOS 8.5.2111** | **CentOS is at EOL.** | **Privilege Escalation (CVE-2020-5291)**  **RCE (CVE-2017-7477)** |
| **CentOS 7 E-comm** | **Local IP: 172.20.241.30**  **Public IP: 172.25.20.34.11** | **CentOS 7** | **00:50:56:9E:72:EA** | **CentOS 8.5.2111** | **CentOS is at EOL.** | **Privilege Escalation (CVE-2020-5291)  RCE (CVE-2017-7477)** |
| **Fedora 21 Webmail/ WebApps** | **Local IP: 172.20.241.40**  **Public IP: 172.25.20.34.39** | **Fedora 21** | **00:50:56:9E:91:10** | **Fedora 37** | **Upgrade to Fedora 37** | **Privilege Escalation (CVE-2015-0278)**  **Buffer Overflow (CVE-2015-2806)** |
| **Palo Alto** | **172.20.242.150** | **PAN OS 10.0.0** | **7C:89:C2:99:12:10** | **PAN OS 11.0.0** | **Upgrade to PAN OS 11.0.0** | **RCE (CVE-2022-0024)**  **RCE (CVE-2021-3061)** |