INTRODUCTION

This project mainly focuses on the documentation and security analysis of devices (8 - 10) that were taken from the college's data center. It also involves in-depth research of two selected devices within the list, outlining the current and potentially recent vulnerabilities that have been discovered and need to be addressed to ensure maximum protection and security of the facility.

The scope of this research covers devices, the software installed on them, and their respective vulnerabilities, which are analyzed in CVE entries published in the past 5 years.

With the increase in recent cybersecurity exposures and breaches within IT security organizations. Routine identification, detection, and updating of system hardware with the most recent software patches are essential to ensure that devices within an organization are safe from security flaws, which can compromise the entire network or even cause financial loss to an organization.

Through this assignment, there'll be an understanding of the current vulnerability issues affecting devices used in an organization, the risk assessment taken on these devices, and practical recommendations, which might include (updating software or physically replacing devices), taken to fix or mitigate these issues. These findings aim to address security issues and contribute to a more secure device practice within the data center.

BRIEFING / METHODOLOGY

Research Method

This assessment was conducted using several methods to ensure comprehensive device reconnaissance and accurate CVE data findings/comparison. Multiple internet sources were employed for these, and a standard evaluation was applied to assess vulnerabilities and their impact

Data Sources

The primary data sources utilized in this assessment include:

1. ATU Data Center:
   Devices were selected with their software versions and system models for documentation and assessment
2. CVE Databases:
   CVE.org, Cvedetails.com, nvd.nist.gov, along with manufacturers websites – These are the primary sources for CVE identifiers, vulnerability descriptions, and their impacts.
3. Device Documentation Sources:
   Various devices with their websites on the internet were used for device description, features, and the possible operating systems that can be installed on them.

Device Selections

The assessment involves 8-10 devices taken from the data center, and listed below are 9 devices to be used for this project. Note that these devices were selected based on their CVE availability:

1. Cisco Nexus 93120 TX
2. Catalyst 2960 – X
3. Fortinet FortiGate 60F
4. Fortinet FortiGate 1500D
5. Fortinet Forti AP 2314
6. DELL Power-Edge M1000 E98
7. DELL R860 XS Server
8. EqualLogic PS4000

Research Parameters

- I searched product names, their installed software, and their CVE identifiers. I also checked for devices with End of Life (EOL) or End of Sale (EOS)
- CVE Date range used: Last outdated version - First CVE vulnerability record, then discussed the most recent CVE

CVSS Scoring

- Common Vulnerability Scoring System: the framework for scoring computer security vulnerabilities from 0 – 10, to help organizations prioritize their vulnerabilities: None (0.0); Low (0.1 – 3.9); Medium (4.0 – 6.9), High (7.0 – 8.9), and Critical (9.0 – 10.0)

Deep Dive Selected Devices

- The 2 listed devices were selected for in-depth analysis because
    - **Catalyst 2960** – X: is a device with End of Sales with no new hardware in production, but still maintaining support until its End of Support in 2027, thereby making it a case study.
    - **Fortinet FortiGate 1500D**: is also a device that has reached both EOL / EOS, and so no recent patch/fix would work for its vulnerabilities.

MAIN BODY

This section shows a table of all 10 devices that were selected for assessment, with their vulnerabilities, and then a detailed analysis of each device with its public CVE vulnerabilities, severity level, and evaluations for their available patches and overall security risks and recommendations.

Devices Overview

Device	Model	Software	CVEs	Recent / Risk score	Most Recent Vulnerability	EOL – EOS / Upgrade fix
Cisco Switch	Cisco Nexus 93120 TX	NX-OS.9.2.4.bin	23	8.8	Python Parser Escape Vulnerability - (CVEdetails.com, 2025)	NX-OS is 10.6(1s)F EOS Device, - (Cisco, 2025)
Cisco Switch	Catalyst2960 – X	15.2(7)E8	67	6.6	An SNMP vulnerability granting an attacker access to cause DOS (CVEdetails.com, 2025)	Device EOL/EOS Cisco IOS XE 17.15.4a (Blumira, 2025)
Firewall Device	Fortinet FortiGate 60F	7.6.4 build 3596 (Feature)	CVE-2024-3596	9.0	RADIUS Protocol under RFC2865 is vulnerable to forgery attacks (NIST, 2025)	FortiAuthenticator 6.6.2 (Fortinet, 2025). Or better use the MS Directory rather than RADIUS.
Firewall Device	Fortinet FortiGate 1500D	V7.2.12 build 1761	12	4.9	API Authenticated Null Pointer Dereference via Crafted Request Leading to HTTP Daemon Crash (CVEdetails.com, 2025)	EOL/EOS 1000F Model
Access Point	Fortinet Forti AP 2314	V 7.6.1 build 0941	16	4.9	API Authenticated Null Pointer Dereference via	Upgrade to 7.6.4 or above

					Crafted Request Leading to HTTP Daemon Crash (CVEdetails.com, 2025)	(FortiGuard Labs, 2025)
Network Server	DELL Power-Edge M1000e	Windows Server 2016	43	9.4 CVE-2025-59287	Remote Code Execution Vulnerability (CVEdetails.com, 2025)	KB5070882 (OS Build 14393.8524) Out-of-band (Microsoft Support, 2025)
Network Server	DELL R860 XS	Ubuntu 22.04.lts	Multiple CVEs	7.8 CVE-2025-40114	Add a check for array bounds in veml6075_read_int_time_ms vulnerability (CVEdetails.com, 2025)	linux-image-6.8.0-86-generic – 6.8.0-86.87~22.04.1 (Canonical Ubuntu Security, 2025)
Storage Arrays	EqualLogic Ps4000	Windows Server 2019	4004	7.5 CVE-2025-59502	Remote Procedure Call Denial of Service Vulnerability (CVEdetails.com, 2025)	[2025-10 Cumulative Update for Windows Server 2019 for x64-based Systems] (Lansweep, 2025)

INDIVIDUAL DEVICE DOCUMENTATION

1. Cisco Nexus 93120 TX: (Cisco, 2025)

Overview:

The Cisco Nexus 93120TX Switch, first announced on Nov 5, 2013, is a high-performance network switch from Cisco designed for both Layer 2 and Layer 3 operations, supporting 10/40 Gigabit Ethernet for data center networks to enable interconnection, virtualization, and automated network management. It can operate in NX-OS mode or Application Centric Infrastructure (ACI) mode, enabling deployment in small businesses, enterprises, and service provider data centers.

EOL Device: (Cisco, 2025)

The device has been declared End of Life on August 31, 2019, by Cisco, and the Last Date of support was February 28, 2025, as referenced in the Reference

Installed NX-OS.9.2.4 software vulnerabilities: (CVEdetails.com, 2025)

- There are 23 CVEs identified from (2019 - 2024).
- The severities are spanned with **1 -** Overflow, being the lowest, and **4** - DOS, the highest.
- The notable vulnerabilities classified for "**most recent/high**"
    - **CVE-2024-20286, CVE-2024-20285, CVE-2024-20284**: (CVSS 8.8) 28/08/24
      A vulnerability that could allow an authenticated, low-privileged, local attacker to escape the Python sandbox and gain unauthorized access to the operating system of the device.

Risk Assessment:
High Risk – it's a serious risk as the attacker will get local root access and all authentication privileges. Meaning that they can tweak the entire device anyhow they can, and if these devices are connected insecurely to other devices, then it becomes a bigger risk to all connected devices.

Potential Solutions

- For non-patch and upgrade to the most recent fixed versions as recommended by Cisco, the **NX-OS is 10.6(1s)F**, which was released on 15 September 2025, for the Cisco Nexus 9000 Series. Or the recent stable version 10.5(4)M, which was updated on 20 October 2025.

- Upgrade to newer model replacement: customers are encouraged to migrate to the Cisco Nexus 93216TC-FX2 Switch (Cisco, 2025)

2. Cisco 2960 – X Switch (Deep Dive Device)

Overview

The Cisco 2960–X Switch, first released on 24th May 2013, is an Ethernet switch designed for campus and branch networks, perfect for medium-sized networks and deployments. It supports Gigabit Ethernet with features like Flex Stack Plus for high-speed stacking, energy efficiency, and other basic modern switching capabilities, and straightforward network management via the Cisco IOS software. **(**Cisco, 2025)

EOL/EOS Device: This device reached EOS on October 31, 2022, as Cisco stopped producing it then, but customers with the device will still be receiving security patches and support until the end of Support on October 31, 2027. (Cisco, 2025)

- There are still firmware security updates from Cisco, as the EOS is still active
- Personally, I'll advise that the device be migrated to a new device in case of hardware issues, as there will be no possible replacement

Recommended Replacements (Cisco, 2025)

- Cisco Catalyst 9200 - 9300 Series, these are the better options. While the Catalyst 9200 series is the direct option, the Catalyst 9300 is best as it has higher performance, stackable, TrustSec, and DNA Center support.

3. Fortinet FortiGate 60F Firewall Device (Cl Social, 2025)

Overview

The Fortinet FortiGate 60F is a portable security firewall device that is designed for small – to medium-sized organizations and branch offices. It offers high-performance threat protection, Firewalling, VPN support, web filtering, application control capabilities, intrusion prevention, and SSL inspection.
It also offers centralized management via Forti Manager and Forti Cloud. With a 10Gbps firewall throughput, it allows high traffic volume with less latency, and a 6.5Gbps VPN throughput, perfect for remote users.

7.6.4 build 3596 (Feature) Vulnerabilities

CVE-2024-3586: NIST (2025). This vulnerability, which was first discovered on July 9, 2024, can allow an attacker to modify a valid RADIUS response to forge another response (e.g., change 'Access-Accept' to 'Access-Reject') using a chosen-prefix collision attack against the MD5 Response Authenticator signature.

Risk Assessment

Since this means that an attacker can modify RADIUS packets sent on a path, tamper with the responses, and potentially change authentication decisions, it is a high-risk vulnerability. The impacts could lead to unauthorized access, session, and packet decision manipulation, Denial of service, and, if this occurs within a connected VLAN, the severity can be high, especially if the attacker has root access.

But the Data Center is not vulnerable to this attack as it uses the Microsoft Directory rather than RADIUS on the device.

Patches:

FortiAuthenticator 6.6.2 was used to update the FortiOS version to v7.4. Series, and the update was automatic and didn't seem like an upgrade to a newer version, though, as seen on the FortiGuard Labs Website. (Fortinet, 2025)

Recommendation

- Update to the fixed patches
- Use the Microsoft Directory in place of RADIUS

4. Fortinet FortiGate 1500D: (Deep Dive Device)

Overview

Unlike the FortiGate 60F, this device is a high-performance firewall for large enterprises and service providers. It offers bigger threat protection and higher firewall throughput (80 Gbps), a VPN throughput of 50 Gbps, and other advanced networking features. However, this device is an EOL/EOS product, which means there is no support or patches for vulnerabilities in versions like FortiOS 7.6.x. Enbitcon (2025)

Features:

- Used to be in demand for fast and high-performance WLAN networks in every organization, FortiAP Access Points provide a secure wireless LAN feature to deploy WLAN quickly and also manage them via the FortiGate firewall, FortiCloud, or via a dedicated WLAN controller.

EOL/EOS Device: Now, this device reached its End of Sale on April 10, 2025, as FortiGate stopped producing it then. The End of Support for Fortinet hardware takes place 60 months after the End of Sale Date.

- There are no more firmware security updates or support from Fortinet
- Because it has been discontinued, it now fails the current cybersecurity compliance requirements

Recommended Replacements

- FortiGate 1000F and the 1800F modes are both solid replacements for the 1500D. The 1000F is faster, while the 1800F has 50% more RAM than the 1000F. (Reddit, 2023)

5. Fortinet FortiAP 2314 Access Point: (Corporate Armor, 2020)

Overview

This device is a Wi-Fi 6 access point device perfect for both small and large organizations, due to its strong performance and low cost. It has 3 radios: 2.4 GHz, 5 GHz, and a separate scanning radio delivering high speed. The Wi-Fi 6 features help open up more lines for endpoints to communicate, so they don't have to wait long for their turn. Fotinet Security adopted it for management, offering advanced security features, and it can now be managed with a FortiGate firewall or FortiAP cloud.

Features

- It has a 2 Gigabit Ethernet port, one supporting Power over Ethernet (PoE), and it also has Bluetooth Low Energy radio for IoT tasks like asset tracking.

V 7.6.1 build 0941 Vulnerabilities

The installed OS has the same recent vulnerability as the V7.2.12 build, since the CVE issue is the most recent generally for Fortinet OS from version 6.4 through 7.6.3. Product not checking the return value, thereby allowing an authenticated user to cause a Null Pointer Deference, crashing the HTTP daemon via a specially crafted request. This vulnerability comes with a 4.9 (medium severity) score. (CVEdetails.com, 2025)

The CVE was discovered on the 14th of October 2025, and it was internally discovered and reported by Loic Panatano of Fortinet PSIRT, as said by the FortiGuard site. (FortiGuard Labs, 2025)

Risk Assessment

Just like I mentioned for the version 7.2.12, if an attacker crashes the HTTP/API daemon, this would disrupt management, and may require reboot or service recovery, causing a lot of impact on the organization, including: Losing remote GUI/API temporarily, delay in operations due to configuration changes, response to incidents, etc.

Fix Recommendation

- First solution is to upgrade to version 7.6.4 or above. (FortiGuard Labs, 2025)
- Limit admin access only to trusted personnel

6. DELL Power-Edge M1000 E98 Server

Overview

Dell PowerEdge M1000e was introduced in 2012, and it's a blade server system perfect for server consolidation. Its design allows for a variety of blade servers, storage, and I/O modules, which makes it a strong base for virtualization and server consolidation. It can accommodate different blade sizes and servers from the 11th to 14th, and its modular size can carry demanding workloads. With a mid-plane update, this chassis has 3 interconnect fabrics, which all support 10GbE speeds. (InfoWorld, 2010)

Windows Server 2016 Vulnerabilities

There was a recorded number of 4345 CVE issues within the WS 2016 version, which has made it so far, the highest number of CVE issues recorded from the devices collected at the data center. This is a range of vulnerabilities from 2016 to 2025. (CVEdetails.com, 2025)

The most recent recorded vulnerability is: CVE-2025-59287, it was discovered on the 14th October, 2025. This causes deserialization of untrusted data in Windows Server Update Service, which allows an unauthorized attacker to execute code over a network. (Microsoft Support, 2025)

Risk Assessment

The attacker doesn't need to be authenticated to run this attack, and it's carried out remotely via the network; all he needs to do is send a specially crafted packet and gain execution as SYSTEM. The threats this can cause are many, for example: Since the attacker has SYSTEM privileges, he can send malicious updates or even modify the system configuration, thereby causing full compromise of the Windows Server. For a large organization, it can lead to breaches of data and exposure.

Recommendation

- Install the KB5070882 (OS Build 14393.8524) Out-of-band update too fix this software issue on the affected devices. (Microsoft Support, 2025)

7. DELL R860 XS Server

Overview
The DELL R860 XS is a rack server with 4 Intel Xeon Scalable Processors. This makes it suitable for high-performance and heavy business tasks like data-intensive applications, machine learning, and rendering etc.
It has a max CPU core count of 60 cores and can support 64 DDR5 DIMMs, which is a total of 16TB of memory. As compared to the R660xs and R760xs, it's cheaper and more power efficient, since they only have 2-core CPUs. (Dell Technologies, 2024)

Ubuntu 22.04. LTS Software Vulnerabilities

There are 3 versions of Ubuntu 22.04.LTS, (noble, jammy, and focal), but we're focusing on the jammy version as it was the one that showed for infecting servers. It's also important to note that Ubuntu 22.04 LTS (Jammy Jellyfish) will reach the end of its standard support in April 2027 and so won't receive support after then.

On cvedetails.com, there was a recorded number of 45 CVE issues in the Ubuntu Linux 22.04 LTS Edition so far, the highest number of CVE issues recorded from the devices collected at the data center. This is a range of vulnerabilities from 2016 to 2024. But on the Linux website, there were vulnerabilities even until 18th April, for Linux 22.04. LTS. (CVEdetails.com, 2025)

The most recent recorded vulnerability is: CVE-2025-40114, it was first seen on 18-04-2025, with a CVSS of 7.8 on the Ubuntu website. This vulnerability issue is an out-of-bounds read

due to a missing array bounds check in veml6075_read_int_time_ms. (Canonical Ubuntu Security, 2025)

Risk Assessment

The impact of this vulnerability is a high impact level because it could lead to the kernel trying to read beyond allocated memory bounds, resulting in a kernel crash.

Recommendation

- Update to the latest package version for the affected 22.04 LTS Jammy as seen on the Ubuntu website:
    - linux-image-6.8.0-86-generic – 6.8.0-86.87~22.04.1 (Canonical Ubuntu Security, 2025)

8. EqualLogic PS4000 Storage Array

Overview

The EqualLogic PS4000 Storage Array iSCSI is a model of storage array with 15k SAS drives, dual controllers, and dual power supplies, making it perfect for small to medium-sized organizations. It also has an online firmware update capability and a centralized management via a console port. With a Windows setup wizard, it's easy to install and manage. It has a high performance when compared to other iSCSI systems in its class, making it perfect for strong VMware virtualization environments. Meanwhile, its GbE ports provide lower throughput.

Windows Server 2019 Software Vulnerabilities

There are 4004 recorded vulnerabilities in the WS 2019 so far, the highest number of CVE issues recorded from the devices collected at the data center. These are a range of vulnerabilities from 2018 to 2025, with Privilege Escalation being the highest. (CVEdetails.com, 2025)

The most recent recorded vulnerability is CVE-2025-59502; it was first seen on 14-10-2025 and has a CVSS score of 7.5. This vulnerability issue is caused by an uncontrolled resource consumption in Windows Remote Procedure Call, allowing an unauthorized attacker to deny service over a network. (Microsoft Support, 2025)

Risk Assessment

An uncontrolled resource-consumption flaw in the Windows Remote Procedure Call (RPC) subsystem allows an unauthorized attacker to send network requests, causing the RPC service to exhaust critical resources (CPU, memory, handles) and triggering a DoS (service disruption). Since many Windows Server roles depend on RPC (Active Directory, file and print services, remote management, WMI, and remote administration), if exploited to cause denial-of-service, they may become unresponsive or unstable, depriving clients and other systems of essential services.

Recommendation

- Install Microsoft's patch as released in the October 2025 Patch Tuesday [2025-10 Cumulative Update for Windows Server 2019 for x64-based Systems] (Lansweep, 2025)
- Better still, upgrade to Windows Server 2025 with the latest upgrades

DEEP DIVE RESULTS

In this section, I am deep-diving into the details of the two listed devices, discussing their current and past known vulnerabilities as shown on the CVE and manufacturer websites, vulnerability and issue assessments, and potential solutions.

a. Catalyst 2960 – X
b. Fortinet FortiGate 1500D

1. **Catalyst 2960 – X:** is a device with End of Sales with no new hardware in production, but still maintaining support until its End of Support in 2027.

15.2(7) E8 (Zero Day) Vulnerabilities:

There are 67 CVEs identified for this Operating System from 2019 to 2025.

- The severities span from 1 - Overflow, being the lowest in the year 2017, to 12 - DOS, the highest in 2025. (CVEdetails.com, *Cisco » IOS » 15.2(7)e8 Operating system*, 2025)

- Most recent vulnerability: CVE-2025-20352 (CVSS 7.7) 24/09/25: (Cisco, 2025)

The Cisco Product Security Incident Response Team (PSIRT) was aware of this vulnerability after a local Administrator's credentials were compromised, and the resolution support case was handled. (Cisco, 2025)

This vulnerability is exploited by sending crafted SNMP packets to an affected device over IPv4 or IPv6 networks. If the attacker has low (user) privileges, they can cause a DOS attack

on the affected device. On the other hand, if he has high (admin) privileges, he can execute this malware as the root user. (Cisco, 2025)

Risk Assessment:

If an attacker exploits this vulnerability, they could execute arbitrary commands as admin, gaining full network-level privileges. The attacker might decide to demand ransoms, since he can easily intercept data via the SNMP access he has. A red hat hacker might decide to crash critical routers/switches, leading to the disconnection of all connected VLANs.

Patches:

Cisco released a maintenance version, Cisco IOS XE Software Release 17.15.4a, on September 24, 2025, and advised that users on this particular OS should update their systems with the patch. (Blumira, 2025)

Recommendation

- Identify devices with outdated OS versions in the data center and update to the most recent fixed versions as recommended by Cisco.
- Since this is an EOD/EOS device, the device has to be changed to an upgraded model, Cisco Catalyst 9300 Series

2. **Fortinet FortiGate 1500D:** is also a device with EOL / EOS, and so no recent patch/fix would work for its vulnerabilities.

V7.2.12 build 1761 Vulnerabilities (CVEdetails.com, 2025)

There are 12 listed vulnerabilities for this OS version, likely because it's old and susceptible to new vulnerabilities.
The most recent is CVE-2025-58903. (CVEdetailss.com *Vulnerability Details: CVE-2025-58903*, 2025). The product does not check the return value, which allows an authenticated user to cause a Null Pointer Deference, thereby crashing the HTTP daemon via a specially crafted request. This vulnerability comes with a 4.9 (medium severity) score.

Risk Assessment
If an attacker crashes the HTTP/API daemon, this would disrupt management and may require reboot or service recovery, and this might cause a lot of impact on the organization,

which might include: Losing remote GUI/API temporarily, delay in operations due to configuration changes, response to incidents, etc. Finally, repeated crashes could lead to a total shutdown.

Device EOS/EOL Status: (Park Place Technologies, 2025)
Since this device has reached its EOS/EOL, using it in the data center poses a security threat, given the vulnerabilities already present in the current software.

Fix Recommendation

- Update OS to the most recent and recommended version (FortiOS 7.6.4 or above): (FortiGuard Labs, 2025)
- Finally, since this is an EOL device, I would recommend changing and upgrading to a higher model, the FortiGate 1000F and 1800F models. Since there's no official statement on which model to upgrade to by Fortinet, I had to get ideas from the communities (Reddit, 2022).

CONCLUSION

Generally, in the assessment of this project, I was able to discover that the major listed vulnerabilities with high impacts were the Denial-of-Service issues, and it was a common CVE in all the devices, although the frequency might vary.

Software manufacturers always release patches for these vulnerabilities within a short period of time; some are even released on the same day the CVEs were detected, and the patches are either automatically updated or a report for the update is posted on the manufacturer's page.

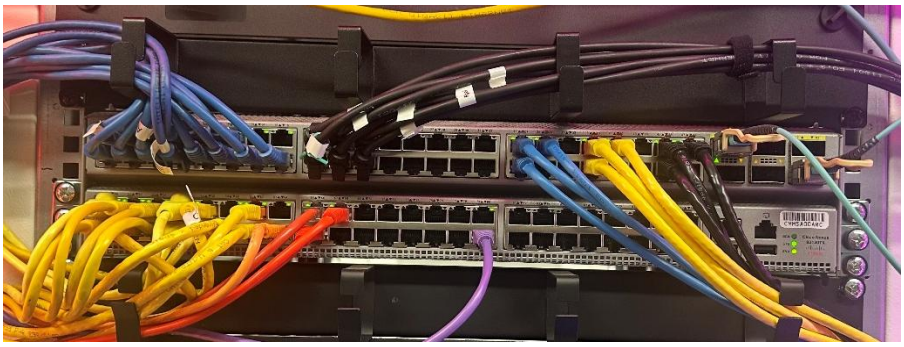
EOD/EOS devices are a risk in every organization because vulnerabilities pile up without a patch, which can cause serious damage, loss of data, or management issues for the organization.

All the devices I used for the case study from the Data Lab have either reached End of Sale, End of Support, or End of Life, or have outdated Operating Systems, which means they are all vulnerable to attacks.

APPENDIX

Image diagrams for the researched devices

1. Cisco Nexus 93120TX Switch



- A high-performance data center switch with 96 fixed 1/10GBASE-T ports and six fixed 40-Gbps QSFP ports, which offers 2.4 TBps of bandwidth Rw4tw.
- Perfect for large data-center networking due to its high bandwidth and port density.

2. Cisco 2960–X Switch

- A stackable Gigabit Ethernet switch with 80 Gbps bandwidth and a dual-core CPU at 600MHz that provides enterprise access for organizations
- Has advanced Cisco IOS Software features like switch hibernation mode.

3. Fortinet FortiGate 60F

- A next-gen firewall device from Fortinet, for small – medium-sized businesses, needed to provide internet security
- Supports intrusion prevention, VPN, application control, SSL inspection, and advanced threat protection with a 10 Gbps throughput.

4. Fortinet FortiGate – 1500D

- A high-performance firewall that offers high-performance threat protection with up to 80 Gbps
- Has the latest FortiASIC NP6 processors and the FortiOS 5 network security platform group security features.

5. Fortinet Forti AP 2314 Firewall

- A Wi-Fi Access Point device with Wi-Fi 6, delivering max throughput 574 Mbps on the 2.4 GHz band and 1.2 Gbps on the 5 GHz band
- It supports WPA3 for future-proofing, with integration from Fortinet Security Fabric for security management.

6. DELL Power-Edge M1000e

- A blade server chassis from DELL, released around 2012.
- Supports blade servers from (11^{th} – 14^{th} Gen) and offers various I/O and switch options.

7. DELL PowerEdge R860 Rack Server

- A Rack server with up to four 4th Generation Intel Xeon Scalable processors with up to 60 cores per processor and optional Intel Quick Assist, which means high-speed processing.

- 64 DDR5 DIMM slots, 16TB max, which means large data/memory handling

8. **EqualLogic PS4000 Storage Array**

   - A 2U iSCSI SAN appliance that supports 8 or 16 SATA drives and dual controllers for fault tolerance.

REFERENCES LIST

Device 1

Cisco (2025) *Cisco Nexus 93120TX*. Available at: https://www.cisco.com/site/us/en/products/networking/cloud-networking-switches/nexus-9000-switches/93120tx/index.html (Accessed: 28 September 2025).

Cisco (2025) *Cisco NX-OS Software Python Sandbox Escape Vulnerabilities.* Available at: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-psbe-ce-YvbTn5du (Accessed: 28 September 2025).

CVE: CVEdetails.com (2025) *Cisco » Nx-os » 9.2(4) (Operating system)*. Available at: https://www.cvedetails.com/version/1630780/Cisco-Nx-os-9.2-4-.html

Cisco (2025) *End-of-Sale and End-of-Life Announcement for the Cisco N9K-C93120TX, N9KC92300YC*. Available at: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/eos-eol-notice-c51-742776.pdf (Accessed: 28 September 2025).

Cisco (2025) *End-of-Sale and End-of-Life Announcement for the Cisco N9K-C93120TX, N9KC92300YC*. Available at: https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/eos-eol-notice-c51-742776.pdf (Accessed: 28 September 2025).

Device 2

Cisco (2025) *Cisco Catalyst 2960-X and 2960-XR Series Switches Data Sheet*. Available at: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/datasheet_c78-728232.html (Accessed: 28 September 2025).

CVEdetails.com (2025) *Vulnerability Details : CVE-2025-20352.* Available at: https://www.cvedetails.com/cve/CVE-2025-20352/ (Accessed: 28 September 2025).

Cisco (2025) *Cisco IOS and IOS XE Software SNMP Denial of Service and Remote Code Execution Vulnerability.* Available at: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte (Accessed: 28 September 2025).

Blumira (Sept 26, 2025) *End-of-Sale and End-of-Life Announcement for the Cisco Catalyst 2960X Product Family*. Available at: https://www.blumira.com/blog/cisco-snmp-zero-day-vulnerability-critical-patch-and-mitigations, (Accessed: 28 September 2025).

Cisco (2025) *Cisco SNMP Zero-Day Vulnerability: Critical Patch and Mitigations*. Available at: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-2960-x-series-switches/eos-eol-notice-c51-744432.html (Accessed: 28 September 2025).

Cisco (2025) *Cisco Catalyst 2960-X Series Switches*. Available at: https://www.cisco.com/c/en/us/support/switches/catalyst-2960-x-series-switches/series.html (Accessed: 28 September 2025).

Device 3

Cl Social (2025) *FortiGate-60F Review: The Perfect Firewall for Small Businesses*. Available at https://social.contadordeinscritos.xyz/blogs/11790/FortiGate-60F-Review-The-Perfect-Firewall-for-Small-Businesses (Accessed: 28 September 2025).

NIST (2025) *CVE-2024-3596 Detail*. Available at https://nvd.nist.gov/vuln/detail/CVE-2024-3596 (Accessed: 28 September 2025).

Fortinet (2025) *RADIUS vulnerability*. Available at https://docs.fortinet.com/document/fortigate/7.6.4/fortios-release-notes/249950 (Accessed: 28 September 2025).

Device 4

Enbitcon (2025) *Fortinet FortiGate 1500D Firewall (End of Sale/Life)*. Available at https://www.enbitcon.ae/shop/fortinet/fortigate-firewall/high-end/fortinet-fortigate-1500d-firewall-end-of-sale-life-fg-1500d (Accessed: 28 September 2025).

CVEdetails.com (2025) *Fortinet » Fortios » 7.2.12.* Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-3080/product_id-6632/version_id-1985114/Fortinet-Fortios-7.2.12.html / CVEdetails.com *Vulnerability Details: CVE-2025-58903.* Available at: https://www.cvedetails.com/cve/CVE-2025-58903/ (Accessed: 28 September 2025).

FortiGuard Labs (2025) *Multiple Unchecked Return Value leading to Null Pointer Dereference.* Available at: https://fortiguard.fortinet.com/psirt/FG-IR-25-653 (Accessed: 29 September 2025).

Park Place Technologies (2025) *FortiGate-1500D-DC.* Available at: https://www.parkplacetechnologies.com/eosl/fortinet/fortigate-1500d-dc/ (Accessed: 29 September 2025).

Achilles_Buffalo (2023) *Upgrading FortiGate's before end of life.* Available at https://www.reddit.com/r/fortinet/comments/12bqfgp/upgrading_fortigates_before_end_of_life/#:~:text=Comments%20Section,80F%20for%20the%2080E%20replacement (Accessed: 29 September 2025).

Device 5

Corporate Armor (2020) *FortiAP 231F – Love that new access point smell.* Available at: https://www.corporatearmor.com/fortiap-231f/fortiap-231f-love-that-new-access-point-smell/ (Accessed: 29 September 2025).

CVEdetails.com (2025) *Fortinet » Fortios » 7.6.1.* Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-3080/product_id-6632/version_id-1915162/year-2025/Fortinet-Fortios-7.6.1.html (Accessed: 29 September 2025).

FortiGuard Labs (2025) *Multiple Unchecked Return Value leading to Null Pointer Dereference.* Available at https://fortiguard.fortinet.com/psirt/FG-IR-25-653 (Accessed: 29 September 2025).

Device 6

InfoWorld (2010) *FortiAP 231F – Blade server review: Dell PowerEdge M1000e.* Available at: https://www.infoworld.com/article/2301783/blade-server-review-dell-poweredge-m1000e.html? (Accessed: 29 September 2025).

CVEdetails.com (2025) *Vulnerability Details: CVE-2025-59287.* Available at: https://www.cvedetails.com/cve/CVE-2025-59287/ (Accessed: 29 September 2025).

Microsoft Support (2025) *October 23, 2025—KB5070882 (OS Build 14393.8524) Out-of-band.* Available at: https://support.microsoft.com/en-us/topic/october-23-2025-kb5070882-os-build-14393-8524-out-of-band-3400c459-db78-48bc-ae69-f61bff15ea7c (Accessed: 29 September 2025).

Device 7

Dell Technologies (2024) *PowerEdge R860.* Available at: https://www.delltechnologies.com/asset/en-ie/products/servers/technical-support/poweredge-r860-spec-sheet.pdf (Accessed: 30 September 2025).

Canonical Ubuntu Security (2025) *CVE-2025-40114.* Available at: https://ubuntu.com/security/CVE-2025-40114; CVEdetails.com (2025) *Canonical » Ubuntu Linux » 22.04 LTS (Operating system)*. Available at: https://www.cvedetails.com/version/703544/Canonical-Ubuntu-Linux-22.04.html (Accessed: 30 September 2025).

Canonical Ubuntu Security (2025) *Ubuntu Security Notices USN-7835-4.* Available at: https://ubuntu.com/security/notices/USN-7835-4 (Accessed: 30 September 2025).

Device 8

TechHead (2025) *Dell EqualLogic PS4000: Hands-on Review Part 1*. Available at: https://techhead.co/dell-equallogic-ps4000-hands-on-review-part-1/ (Accessed: 30 September 2025).

CVEdetails.com (2025) *Microsoft » Windows Server 2019: Security Vulnerabilities, CVEs*. Available at: https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-50662/Microsoft-Windows-Server-2019.html?page=1&order=1 (Accessed: 30 September 2025).

Microsoft Support (2025) *Remote Procedure Call Denial of Service Vulnerability.* Available at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-59502 (Accessed: 30 September 2025).

Lansweeper (2025) *Microsoft Patch Tuesday – October 2025.* Available at https://www.lansweeper.com/blog/patch-tuesday/microsoft-patch-tuesday-october-2025/?utm_source=chatgpt.com (Accessed: 30 September 2025).