Advisory Alert

Alert Number: AAA20250722 **Date:** July 22, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Sophos	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities
F5	**Medium**	Certificate Validation Bypass Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-50602, CVE-2024-2961, CVE-2024-52533, CVE-2023-6780, CVE-2025-26466)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Precision Rack iDRAC9 firmware. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Precision 7920 Rack iDRAC9 firmware versions prior to 7.00.00.181 Precision 7920 XL Rack iDRAC9 firmware versions prior to 7.00.00.181 Precision 7960 Rack iDRAC9 firmware versions prior to 7.20.30.50 Precision 7960 XL Rack iDRAC9 firmware versions prior to 7.20.30.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000306810/dsa-2025-179

Affected Product	**Sophos**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6704, CVE-2025-7624, CVE-2025-7382, CVE-2024-13974, CVE-2024-13973)
Description	Sophos has released security updates addressing multiple vulnerabilities that exist in Sophos Firewalls. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, SQL Injection and Command Injection. Sophos advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Sophos Firewall versions prior to v21.5 GA (21.5.0)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.sophos.com/en-us/security-advisories/sophos-sa-20250721-sfos-rce

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-52999, CVE-2024-57980, CVE-2024-58002, CVE-2025-21905, CVE-2025-37958, CVE-2025-38089)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:11474 • https://access.redhat.com/errata/RHSA-2025:11428 • https://access.redhat.com/errata/RHSA-2025:11411

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-30102, CVE-2025-30101, CVE-2025-30477, CVE-2024-45333, CVE-2024-36292, CVE-2024-45371, CVE-2024-47800, CVE-2024-46895, CVE-2024-28954, CVE-2024-29222, CVE-2024-39758, CVE-2024-31150, CVE-2024-43101, CVE-2024-45067, CVE-2025-20052, CVE-2025-20101, CVE-2025-20018, CVE-2025-20003, CVE-2025-21099, CVE-2025-20041, CVE-2025-20071, CVE-2025-20031, CVE-2025-20104, CVE-2025-20108, CVE-2025-20015, CVE-2025-20629)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerEdge Server and PowerScale OneFS. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale OneFS versions 9.4.0.0 through 9.10.1.0 PowerScale OneFS version 9.7.0.0 through 9.7.1.7 PowerScale OneFS versions 9.8.0.0 through 9.10.1.0 PowerScale OneFS versions prior to 9.11.0.0 PowerEdge Server Intel E810 Adapters and Intel E823 LOM Firmware versions prior to 24.0.0 PowerEdge Server Intel I350 and X550 Adapters Firmware versions prior to 24.0.0 PowerEdge Server Intel X710, XXV710, and XL710 Adapters Firmware versions prior to 24.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000347891/dsa-2025-198-dell-poweredge-server-security-update-for-intel-ethernet-controllers-adapters-and-intel-data-center-gpu-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000317419/dsa-2025-192-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Certificate Validation Bypass Vulnerability (CVE-2024-45341)
Description	F5 has released security updates addressing a Certificate Validation Bypass Vulnerability that exists in F5OS. **CVE-2024-45341** - A certificate with a URI which has an IPv6 address with a zone ID may incorrectly satisfy a URI name constraint that applies to the certificate chain. Certificates containing URIs are not permitted in the web PKI, so this only affects users of private PKIs which make use of URIs. This vulnerability may allow a remote attacker to gain access to or modify sensitive data on the system. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A version 1.8.0 F5OS-C versions 1.8.0 - 1.8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000152658

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.