Advisory Alert

Alert Number: AAA20250304 **Date:** March 4, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
F5	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Cross-site Scripting Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0509, CVE-2025-21502, CVE-2022-23830, CVE-2023-20521, CVE-2023-20526, CVE-2023-20592, CVE-2022-23820, CVE-2023-46218, CVE-2023-46219, CVE-2022-2068, CVE-2022-1292, CVE-2016-2108, CVE-2016-0702, CVE-2016-0705, CVE-2016-0797, CVE-2016-0798, CVE-2016-0799, CVE-2016-0800)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Data Protection Search and IDPA. 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	• Dell Data Protection Search versions 19.6.0, 19.6.1, 19.6.2, 19.6.3, 19.6.4, 19.6.5 running on SLES 12 SP5 • Dell Integrated Data protection Appliance (IDPA) versions 2.7.8 or below running on SLES 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000290991/dsa-2025-109-security-update-for-dell-data-protection-search-for-multiple-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4244, CVE-2023-52923, CVE-2024-35863, CVE-2024-50199, CVE-2024-53104, CVE-2024-56600, CVE-2024-56601, CVE-2024-56623, CVE-2024-56650, CVE-2024-56658, CVE-2024-56664, CVE-2024-56759, CVE-2024-57791, CVE-2024-57798, CVE-2024-57849, CVE-2024-57893)
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	openSUSE Leap 15.3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux SUSE Linux Enterprise Server 15 SP3 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20250771-1/

Affected Product	**F5**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-39573, 2024-38474, CVE-2024-38475, CVE-2025-1695, CVE-2015-3166, CVE-2024-25062, CVE-2023-38709, CVE-2022-40304, CVE-2022-43680, CVE-2024-24795, CVE-2024-21782, CVE-2020-14314)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Information Disclosure, Denial-Of-Service, code or script execution, data modification. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions 17.0.0 - 17.1.2, 16.1.0 - 16.1.3 and 15.1.0 - 15.1.8 BIG-IP (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO) versions 16.0.0 - 16.0.1 F5OS-A versions 1.7.0 and 1.5.1 - 1.5.2 F5OS-C versions 1.6.0 - 1.6.2 NGINX Unit versions 1.29.1 - 1.34.1 Traffix SDC 5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000140693 • https://my.f5.com/manage/s/article/K000140620 • https://my.f5.com/manage/s/article/K000149959 • https://my.f5.com/manage/s/article/K000150204 • https://my.f5.com/manage/s/article/K000141357 • https://my.f5.com/manage/s/article/K000139764 • https://my.f5.com/manage/s/article/K000132686 • https://my.f5.com/manage/s/article/K000139594 • https://my.f5.com/manage/s/article/K000139525 • https://my.f5.com/manage/s/article/K000139447 • https://my.f5.com/manage/s/article/K98606833 • https://my.f5.com/manage/s/article/K67830124

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Cross-site Scripting Vulnerability (CVE-2024-10234)
Description	Red Hat has released security updates addressing a Cross-site Scripting Vulnerability that exists in JBoss Enterprise Application Platform. **CVE-2024-10234** - A vulnerability was found in Wildfly, where a user may perform Cross-site scripting in the Wildfly deployment system. This flaw allows an attacker or insider to execute a deployment with a malicious payload, which could trigger undesired behavior against the server. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 9 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:2029 • https://access.redhat.com/errata/RHSA-2025:2026

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.