Advisory Alert

Alert Number: AAA20250225 **Date:** February 25, 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
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities
F5	**Medium**, **Low**	Tcpdump Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical** - Initial release date **June 26, 2024 (AAA20240626)**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-11979, CVE-2021-36374, CVE-2023-34149, CVE-2023-34396, CVE-2023-41835, CVE-2023-50164, CVE-2023-41900, CVE-2017-18640, CVE-2014-9515)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Avamar products. 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 Avamar operating system versions 19.4, 19.7,19.8,19.9 and 19.10 running on • Dell Avamar Data Store Gen5A, Gen4T • Avamar Virtual Edition for VMware ESXi and vSphere • Avamar Virtual Edition for VMware vSphere • Avamar Virtual Edition for Hyper-V 2012 • Avamar Virtual Edition for Hyper-V 2012R2, Hyper-V 2016, and Hyper-V 2019 • Avamar Virtual Edition for KVM/Open Stack KVM Dell Avamar operating system versions 2.7.0 through 2.7.6 running on Dell PowerProtect DP Series Appliance (Integrated Data Protection Appliance)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226407/dsa-2024-280-security-update-for-dell-avamar-and-dell-avamar-virtual-edition-multiple-security-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-36974, CVE-2024-40956, CVE-2024-53104, CVE-2024-35789)
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, 15.4, 15.5, 15.6 SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250703-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250704-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250698-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250687-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52425, CVE-2024-53908, CVE-2024-53907, CVE-2023-52426, CVE-2022-29162, CVE-2023-25809, CVE-2023-27561, CVE-2023-28642, CVE-2024-21626, CVE-2024-56201, CVE-2024-56326, CVE-2022-48468, CVE-2024-45491)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Storage Defender Resiliency Service. Exploitation of these vulnerabilities may lead to Denial of Service, SQL Injection, Privilege Escalation, Bypass Security Restrictions and Arbitrary Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Resiliency Service versions 2.0.0 - 2.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7183145

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux Kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7288-1

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24852, CVE-2024-36274, CVE-2024-36293, CVE-2024-39279, CVE-2024-28047)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell products. 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, 7920 XL Rack, Precision 7960 Rack and Precision 7960 XL Rack - Intel-I350-X550-X710-E810-Ethernet-Controller-Driver versions prior to 24.3.0.0 • Precision 7920 Rack and 7920 XL Rack - BIOS versions prior to 2.23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000244470/dsa-2025-008

Affected Product	**F5**
Severity	**Medium**, **Low**
Affected Vulnerability	Tcpdump Vulnerability (CVE-2020-8037)
Description	F5 has released security updates addressing a Tcpdump Vulnerability that exists in BIG-IP and F5OS modules. This flaw allows a remote attacker to send specially crafted packets that, when printed, can lead the application to allocate a large amount of memory, resulting in a denial-of-service (DoS). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP versions 17.1.0 - 17.1.2, 16.1.0 - 16.1.5 and 15.1.0 - 15.1.10 F5OS-A versions 1.8.0 and 1.5.1 - 1.5.2 F5OS-C versions 1.6.0 - 1.6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000149929

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.