Advisory Alert

Alert Number: **AAA20250624** **Date:** **June 24, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
Dell	**High**, **Medium**, **Low**	Multiple Vulnerabilities
FortiGuard	**Medium**	Buffer Overflow Vulnerability
F5	**Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Linux kernel vulnerabilities
Hitachi	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exists in Third Party products which intern affect Dell VxRail Appliance. These vulnerabilities that 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 VxRail Appliance Versions - 8.0.000 through 8.0.330
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000335212/dsa-2025-244-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	SUSE
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities (CVE-2024-40937, CVE-2024-50124, CVE-2024-50125, CVE-2024-50127, CVE-2024-50257, CVE-2024-50279, CVE-2024-50301, CVE-2024-53208, CVE-2024-56582, CVE-2024-56601, CVE-2024-56605)
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in Their products. These vulnerabilities could be exploited by malicious users to cause out-of-bounds access and use-after-free. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-202502069-1/

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing Multiple Vulnerabilities that exist in Their products. These vulnerabilities that 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	Connectrix B-Series FOS Versions - prior to 9.2.2 Connectrix B-Series SANnav Versions - prior to 2.4.0 Dell Policy Manager for Secure Connect Gateway Versions - prior to 5.28.00.14 PowerEdge T40 BIOS Versions - prior to 1.19.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000334535/dsa-2025-230-security-update-for-dell-connectrix-b-series-brocade-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000335109/dsa-2025-249-security-update-for-dell-secure-connect-gateway-policy-manager-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000335070/dsa-2025-254-security-update-for-dell-poweredge-t40-mini-tower-server-for-an-improper-link-resolution-vulnerability • https://www.dell.com/support/kbdoc/en-us/000335106/dsa-2025-256-security-update-for-dell-poweredge-t40-mini-tower-server-for-tianocore-edk2-vulnerability • https://www.dell.com/support/kbdoc/en-us/000335103/dsa-2025-255-security-update-for-dell-poweredge-t40-mini-tower-server-for-multiple-ami-bios-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000335060/dsa-2025-252-security-update-for-dell-poweredge-t40-mini-tower-server-for-a-security-version-number-mutable-to-older-versions-vulnerability

Affected Product	**FortiGuard**	
Severity	Medium	
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2024-26010)	
Description	FortiGuard has released security updates addressing buffer overflow vulnerability that exists in Their products. **CVE-2024-26010** - A stack-based overflow vulnerability [CWE-124] in FortiOS, FortiProxy, FortiPAM and FortiSwitchManager may allow a remote attacker to execute arbitrary code or command via crafted packets reaching the fgfmd daemon, under certain conditions which are outside the control of the attacker. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.	
Affected Products	FortiOS 6.4 Versions - 6.4 all versions FortiOS 6.2 Versions - 6.2 all versions FortiOS 6.0 Versions - 6.0 all versions FortiPAM 1.2 Versions - 1.2 all versions FortiPAM 1.1 Versions - 1.1 all versions FortiPAM 1.0 Versions - 1.0 all versions FortiProxy 2.0 Versions - 2.0 all versions FortiProxy 1.2 Versions - 1.2 all versions FortiProxy 1.1 Versions - 1.1 all versions	FortiProxy 1.0 Versions - 1.0 all versions FortiOS 7.4 Versions - 7.4.0 through 7.4.3 FortiOS 7.2 Versions - 7.2.0 through 7.2.7 FortiOS 7.0 Versions - 7.0.0 through 7.0.14 FortiProxy 7.4 Versions - 7.4.0 through 7.4.3 FortiProxy 7.2 Versions - 7.2.0 through 7.2.9 FortiProxy 7.0 Versions - 7.0.0 through 7.0.16 FortiSwitchManager 7.2 Versions - 7.2.0 through 7.2.3 FortiSwitchManager 7.0 Versions - 7.0.1 through 7.0.3
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-24-036	

Affected Product	**F5**
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45310)
Description	F5 has released security updates addressing remote code execution that exist in Their products. **CVE-2024-45310** - An authenticated local attacker could exploit this vulnerability through OpenTelemetry (OTEL) collectors. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next SPK Versions - 2.0.0 - 2.0.1, 1.7.0 - 1.9.2 BIG-IP Next CNF Versions - 2.0.0 - 2.0.1, 1.1.0 - 1.4.1 BIG-IP Next for Kubernetes - 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000151924

Affected Product	**Ubuntu**
Severity	Medium
Affected Vulnerability	Multiple Linux kernel vulnerabilities (CVE-2025-39735, CVE-2025-39728, CVE-2025-38637, CVE-2025-38575, CVE-2025-38152, CVE-2025-37937, CVE-2025-37889, CVE-2025-37785, CVE-2025-23138, CVE-2025-23136)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Their products. These vulnerabilities that 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 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7591-1

Affected Product	**Hitachi**
Severity	Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38709, CVE-2024-24795, CVE-2024-27316, CVE-2024-2511, CVE-2024-38476, CVE-2024-38473, CVE-2024-38477, CVE-2025-21587, CVE-2025-30698)
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in Their products. These vulnerabilities that could be exploited by malicious users to compromise the affected system. Hitachi 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.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2025-101/index.html#vuln • https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2025-102/index.html • https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2025-103/index.html • https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2025-104/index.html • https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2025-105/index.html • https://www.hitachi.com/products/it/software/security/info/vuls/hitachi-sec-2025-117/index.html#product

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.