TLP: WHITE

Advisory Alert

Alert Number: **AAA20250314** **Date:** **March 14, 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
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Dell	**Medium**	Open Redirect Vulnerability
Juniper	**Medium**	Improper Isolation or Compartmentalization vulnerability
Synology	**Medium**	Multiple Vulnerabilities
PHP	**Medium**	Multiple Vulnerabilities
FortiGuard	**Medium**, **Low**	Multiple Vulnerabilities
Palo Alto Networks	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affect Dell VxRail Appliance. 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 VxRail Appliance versions prior to 8.0.322
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000294363/dsa-2025-115-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

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	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 openSUSE Leap 15.3, 15.5, 15.6 Public Cloud Module 15-SP6 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP3, 15 SP6 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.5 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP3, 15 SP6 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, 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6 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-20250847-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250853-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250855-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250856-1/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20141, CVE-2025-20143, CVE-2025-20146, CVE-2025-20142, CVE-2025-20138, CVE-2025-20177, CVE-2025-20144, CVE-2025-20145, CVE-2025-20115)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service, Privilege Escalation, bypass verifications, configurations and security restrictions. Cisco 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xrike-9wYGpRGq • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xr792-bWfVDPY • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-lkm-zNErZjbZ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-multicast-ERMrSvq7 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv4uni-LfM3cfBu • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-priv-esc-GFQjxvOF • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xr-verii-bypass-HhPwQRvx • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ncs-hybridacl-crMZFfKQ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-modular-ACL-u5MEPXMm • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-bgp-dos-O7stePhX

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Open Redirect Vulnerability (CVE-2025-21104)
Description	Dell has released security updates addressing an Open Redirect Vulnerability that exists in Dell NetWorker Management Console. **CVE-2025-21104** - An unauthenticated attacker with remoter access could potentially exploit this vulnerability, leading to a targeted application user being redirected to arbitrary web URLs. The vulnerability could be leveraged by attackers to conduct phishing attacks that cause users to divulge sensitive information. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetWorker Management Console versions prior to 19.11.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000294392/dsa-2025-124-security-update-for-dell-networker-management-console-for-http-host-header-injection-vulnerability

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Improper Isolation or Compartmentalization vulnerability (CVE-2025-21590)
Description	Juniper has released security updates addressing an Improper Isolation or Compartmentalization vulnerability that exists in Junos OS. **CVE-2025-21590** - An Improper Isolation or Compartmentalization vulnerability in the kernel of Juniper Networks. A local attacker with access to the shell is able to inject arbitrary code which can compromise an affected device. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS versions: 21.4 versions before 21.4R3-S10 22.2 versions before 22.2R3-S6 22.4 versions before 22.4R3-S6 23.2 versions before 23.2R2-S3 24.2 versions before 24.2R1-S2, 24.2R2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2025-03-Out-of-Cycle-Security-Bulletin-Junos-OS-A-local-attacker-with-shell-access-can-execute-arbitrary-code-CVE-2025-21590?language=en_US

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-29843, CVE-2025-29844, CVE-2025-29845, CVE-2025-29846)
Description	Synology has released security updates addressing multiple vulnerabilities that exist in Synology Router Manager. These vulnerabilities could be exploited by malicious users to compromise the affected system. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SRM 1.3 versions prior to 1.3.1-9346-13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_25_04

Affected Product	**PHP**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1219, CVE-2025-1736, CVE-2025-1861, CVE-2025-1734, CVE-2025-1217, CVE-2024-11235)
Description	PHP 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. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP versions prior to: 8.1.32 8.2.28 8.3.18 8.4.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.php.net/ChangeLog-8.php#8.2.28 • https://www.php.net/ChangeLog-8.php#8.1.32 • https://www.php.net/ChangeLog-8.php#8.4.5 • https://www.php.net/ChangeLog-8.php#8.3.19

Affected Product	**FortiGuard**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42784, CVE-2024-55594, CVE-2024-52963)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in FortiWeb and FortiOS. Exploitation of these vulnerabilities may lead to Denial of Service, unauthorized code or commands execution, and web firewall protection bypass. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiWeb 7.4 versions 7.4.0 through 7.4.6 FortiWeb 7.2 all versions FortiWeb 7.0 all versions FortiOS 7.6.0 FortiOS 7.4 versions 7.4.0 through 7.4.7 FortiOS 7.2 versions 7.2.0 through 7.2.10 FortiOS 7.0 all versions FortiOS 6.4 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-23-115 • https://www.fortiguard.com/psirt/FG-IR-24-373

Affected Product	**Palo Alto Networks**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0114, CVE-2025-0115, CVE-2025-0116, CVE-2025-0117, CVE-2025-0118)
Description	Palo Alto Networks has released security updates addressing multiple vulnerabilities that exist in PAN-OS and GlobalProtect App. Exploitation of these vulnerabilities may lead to Denial of Service, Local Privilege Escalation, read arbitrary files. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2 versions prior to 11.2.5 PAN-OS 11.1 versions prior to 11.1.8 PAN-OS 11.0 versions prior to 11.0.6 PAN-OS 10.2 versions prior to 10.2.13-h5 PAN-OS 10.2 versions prior to 10.2.14 PAN-OS 10.1 versions prior to 10.1.14-h11 GlobalProtect App 6.3 versions prior to 6.3.3 on Windows GlobalProtect App 6.2 versions prior to 6.2.6 on Windows GlobalProtect App 6.1 all versions on Windows GlobalProtect App 6.0 all versions on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2025-0114 • https://security.paloaltonetworks.com/CVE-2025-0115 • https://security.paloaltonetworks.com/CVE-2025-0116 • https://security.paloaltonetworks.com/CVE-2025-0117 • https://security.paloaltonetworks.com/CVE-2025-0118

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.