Advisory Alert

Alert Number: AAA20250417 **Date:** April 17, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Double Free Vulnerability
Ubuntu	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
SonicWall	**Medium**	Improper Link Resolution vulnerability
Palo Alto	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities in the Dell PowerProtect Cyber Recovery and Dell ObjectScale 4.0 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	PowerProtect Cyber Recovery Software Versions 19.13.0 through 19.19.0 Dell ObjectScale Versions prior to 4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000306005/dsa-2025-113-security-update-for-dell-powerprotect-cyber-recovery • https://www.dell.com/support/kbdoc/en-us/000300068/dsa-2025-097-security-update-for-dell-objectscale-4-0-multiple-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Double Free Vulnerability (CVE-2022-49541)
Description	Red Hat has released security updates addressing Double Free Vulnerability that exist in their products. **CVE-2022-49541 –** This is a kernel live patch module which can be loaded by the kpatch command line utility to modify the code of a running kernel. This patch module is targeted for kernel-5.14.0-70.85.1.el9_0. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:3961

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0995, CVE-2024-26928, CVE-2024-35864, CVE-2024-50302, CVE-2024-53063, CVE-2024-56595, CVE-2024-56672, CVE-2024-57798)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to compromise systems. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 LTS Ubuntu 22.04 LTS Ubuntu 20.04 LTS Ubuntu 18.04 ESM Ubuntu 16.04 ESM Ubuntu 14.04 ESM
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0111-1

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20236, CVE-2025-20178, CVE-2025-20150)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco Webex App Client and Cisco Secure Network Analytics products. **CVE-2025-20236** – This vulnerability in the custom URL parser of Cisco Webex App could allow an unauthenticated, remote attacker to persuade a user to download arbitrary files, which could allow the attacker to execute arbitrary commands on the host of the targeted user. **CVE-2025-20178** – This vulnerability in the web-based management interface of Cisco Secure Network Analytics could allow an authenticated, remote attacker with valid administrative credentials to execute arbitrary commands as root on the underlying operating system. **CVE-2025-20150** – This vulnerability in Cisco Nexus Dashboard could allow an unauthenticated, remote attacker to enumerate LDAP user accounts. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Webex App Versions 44.6 , 44.7 Secure Network Analytics Versions 7.5.0 to 7.5.2 Secure Network Analytics Data Store Secure Network Analytics Flow Collector Secure Network Analytics Flow Sensor Secure Network Analytics Manager Secure Network Analytics UDP Director Secure Network Analytics Virtual Data Store Secure Network Analytics Virtual Flow Collector Secure Network Analytics Virtual Flow Sensor Secure Network Analytics Virtual Manager Secure Network Analytics Virtual UDP Director Cisco Nexus Dashboard Versions 3.1 and earlier Cisco Nexus Dashboard Version 3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-app-client-rce-ufyMMYLC • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-prvesc-4BQmK33Z • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nd-unenum-2xFFh472

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Improper Link Resolution vulnerability (CVE-2025-32817)
Description	SonicWall has released security updates addressing an Improper Link Resolution vulnerability that exists in SonicWall connect tunnel Windows Client module. **CVE-2025-32817** A Improper Link Resolution vulnerability in the SonicWall Connect Tunnel Windows (32 and 64 bit) Client, this results in unauthorized file overwrite, potentially leading to denial of service or file corruption. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Connect Tunnel Windows (32 and 64 bit) Client 12.4.3.283 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0007

Affected Product	**Palo Alto**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0125, CVE-2025-0122)
Description	Palo Alto has released security updates addressing a improper input neutralization vulnerability and A denial-of-service (DoS) vulnerability that exists Products. **CVE-2025-0125** - An improper input neutralization vulnerability in the management web interface of the Palo Alto Networks PAN-OS® software enables a malicious authenticated read-write administrator to impersonate another legitimate authenticated PAN-OS administrator. **CVE-2025-0122** - A denial-of-service (DoS) vulnerability in Palo Alto Networks Prisma® SD-WAN ION devices enables an unauthenticated attacker in a network adjacent to a Prisma SD-WAN ION device to disrupt the packet processing capabilities of the device by sending a burst of crafted packets to that device. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 11.2 < 11.2.5 PAN-OS 11.1 < 11.1.5 PAN-OS 11.0 < 11.0.6 PAN-OS 10.2 < 10.2.11 PAN-OS 10.1 < 10.1.14-h11 Prisma SD-WAN 6.5 < 6.5.1 Prisma SD-WAN 6.4 < 6.4.2 Prisma SD-WAN 6.3 < 6.3.4 Prisma SD-WAN 6.2 Prisma SD-WAN 6.1 < 6.1.10 Prisma SD-WAN 5.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.paloaltonetworks.com/CVE-2025-0125 • https://security.paloaltonetworks.com/CVE-2025-0122

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.