Advisory Alert

Alert Number: AAA20260702 **Date:** July 2, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
Ubuntu	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29371, CVE-2025-13465, CVE-2025-58056, CVE-2026-1002, CVE-2026-4800, CVE-2026-6860, CVE-2026-23864, CVE-2026-24281, CVE-2026-24308, CVE-2026-27980, CVE-2026-33870, CVE-2026-33871, CVE-2026-34480, CVE-2026-39852, CVE-2026-41240, CVE-2026-42044, CVE-2026-42583, CVE-2026-42587, CVE-2026-44249, CVE-2026-44573, CVE-2026-44574, CVE-2026-44575, CVE-2026-44577, CVE-2026-44578, CVE-2026-44579, CVE-2026-44893, CVE-2026-45109, CVE-2026-45416, CVE-2026-45674, CVE-2026-47691, CVE-2026-48043, CVE-2026-48059, CVE-2026-2614, CVE-2026-33245, CVE-2026-34993, CVE-2026-48710, CVE-2026-5241, CVE-2026-8643, CVE-2026-50010, CVE-2026-50559)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat JBoss Middleware 1 x86_64 Red Hat OpenShift AI
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:34456 • https://access.redhat.com/errata/RHSA-2026:34608

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-34282, CVE-2026-22003, CVE-2026-22021, CVE-2026-22008, CVE-2026-22018, CVE-2026-22007, CVE-2026-34268, CVE-2026-20652)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Data Protection Advisor Versions 19.9 through 19.12 SP2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000483949/dsa-2026-306-security-update-for-dell-data-protection-advisor-for-jdk-8u481-vulnerabilities

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20213, CVE-2026-20214, CVE-2026-20215, CVE-2026-20216, CVE-2026-20217, CVE-2026-20191, CVE-2026-20243, CVE-2026-20244)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco Catalyst Center affects all deployments Secure Endpoint Connector for Windows/Linux/Mac
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-catc-file-read-wLH2vf8X

Vendor	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu Versions 26.04 LTS, 25.10, 24.04 LTS, 22.04 LTS and 20.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8493-1 • https://ubuntu.com/security/notices/USN-8492-1 • https://ubuntu.com/security/notices/USN-8488-1 • https://ubuntu.com/security/notices/USN-8490-1

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 Public Cloud Module 15-SP7 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262722-1/

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.