Advisory Alert

Alert Number: AAA20260820 **Date:** August 20, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Drupal	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Metro node versions prior to 9.2 RecoverPoint for Virtual Machines running: • Debian 12 versions 6.0.3 and 6.0.3.1 • SUSE Linux Enterprise Server 15 SP6 versions prior to 6.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000501900/dsa-2026-372-security-update-for-dell-vplex-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000501664/dsa-2026-096-security-update-for-dell-recoverpoint-for-virtual-machines-multiple-vulnerabilities

Vendor	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20030, CVE-2026-20357, CVE-2026-20358, CVE-2026-20359, CVE-2026-20231, CVE-2026-20315, CVE-2026-20317, CVE-2026-20318, CVE-2026-20319)
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 Crosswork versions 7.2.1 and earlier Cisco Secure Workload Software as a Service (SaaS) versions 3.10, 4.0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-crosswork-UzDTU9Vh • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-csw1-shSvndWP

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-5222, CVE-2025-10263, CVE-2025-40026, CVE-2026-2291, CVE-2026-14474, CVE-2026-14476, CVE-2026-43038, CVE-2026-43125, CVE-2026-43329, CVE-2026-64530, CVE-2024-42516, CVE-2024-43204, CVE-2026-1965, CVE-2026-3783, CVE-2026-3784, CVE-2026-6253, CVE-2026-7168, CVE-2026-8286, CVE-2026-8458, CVE-2026-8924, CVE-2026-8927, CVE-2026-8932, CVE-2026-9079, CVE-2026-9545, CVE-2026-9547, CVE-2026-10536, CVE-2026-12064, CVE-2026-24072, CVE-2026-29167, CVE-2026-29170, CVE-2026-34355, CVE-2026-34356, CVE-2026-42356, CVE-2026-42535, CVE-2026-42536, CVE-2026-43951, CVE-2026-44119, CVE-2026-44185, CVE-2026-44186, CVE-2026-44631, CVE-2026-48913)
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 Core Services Text-Only Advisories: x86_64 Red Hat Enterprise Linux 8.8 (Extended Life Cycle Long Life, Update Services for SAP Solutions): x86_64, ppc64le Red Hat OpenShift Container Platform 4.18 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x Red Hat OpenShift Container Platform 4.19 (RHEL 8 / RHEL 9): x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:54553 https://access.redhat.com/errata/RHSA-2026:54544 https://access.redhat.com/errata/RHSA-2026:55761 https://access.redhat.com/errata/RHSA-2026:56869

Vendor	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76759, CVE-2026-76782, CVE-2026-76758, CVE-2026-76755, CVE-2026-76756, CVE-2026-76757)
Description	Drupal 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. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Drupal End of Support Modules: • Gammu SMS Daemon (all versions) • Link content parser (all versions) • Screenshot (all versions)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-102 https://www.drupal.org/sa-contrib-2026-101 https://www.drupal.org/sa-contrib-2026-100

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0938, CVE-2025-47273, CVE-2025-13836, CVE-2025-31115, CVE-2025-50181, CVE-2026-26950, CVE-2026-31431, CVE-2026-43284, CVE-2026-43500, CVE-2026-46300, CVE-2026-46333, CVE-2025-61984, CVE-2025-61985, CVE-2026-35385, CVE-2026-35386, CVE-2026-35387, CVE-2026-35388, CVE-2026-35414, CVE-1999-0511, CVE-2026-49503, CVE-2026-49504)
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	Dell UCC Edge versions prior to 3.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000501633/dsa-2026-246-security-update-for-dell-ucc-edge-multiple-vulnerabilities

Vendor	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-57819, CVE-2026-54225, CVE-2026-64958)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-57819:** Apache CXF allows to set a limit on the number of form parameters in a JAX-RS message via the "maxFormParameterCount" configuration option. However, no default limit is set which may lead to denial of service attacks when processing requests with very large numbers of form parameters. **CVE-2026-54225:** Apache CXF allows to control the maximum attachment size via the "attachment-max-size". Prior to Apache CXF 4.2.3 and 4.1.8 and 3.6.12, there was no default placed on this size, meaning that a denial of service attack is possible if the user doesn't explicitly set the limit. **CVE-2026-64958:** An incomplete fix for CVE-2026-50645 continues to allow a possible a denial of service attack on Apache CXF by sending a message with many attachment headers. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server versions 8.5, 9.0, and 9.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7284282

Vendor	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20320, CVE-2026-20314, CVE-2026-20302, CVE-2026-20177, CVE-2026-20232, CVE-2026-20327)
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 BroadWorks: • Application Delivery Platform versions prior to RI.2026.071 • Application Server versions prior to RI.2026.07 • Profile Server versions prior to RI.2026.07 • Xtended Services Platform versions prior to RI.2026.07 Cisco Packaged CCE and Unified CCE versions 15.0 and prior Cisco RoomOS versions 20, 11 and prior Cisco IE 1000 Series Switches versions 1.9 and prior Cisco Unified Intelligence Center Software versions 15.0, 12.6 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bworks-xxe-uwUd7CEt • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucce-pcce-ssrf-TghHxD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-bof-vTMANZgu • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ie1k-uxq86Lnx • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ie1k-NgXUFF52 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-sql-inject-2qbfWSm5

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.