Advisory Alert

Alert Number: AAA20260226 **Date:** February 26, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Buffer-Overflow Vulnerability
Cisco	**Critical**	Authentication Bypass Vulnerabilities
Dell	**High**	Denial of Service Vulnerability
Drupal	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer-Overflow Vulnerability (CVE-2026-1188)
Description	IBM has released security updates addressing a vulnerability that exists in their DB2 Recovery Expert Products. **CVE-2026-1188 -** Due to missing input sanitation, SAP Solution Manager allows an authenticated attacker to insert malicious code when calling a remote-enabled function module. This could provide the attacker with full control of the system hence leading to high impact on confidentiality, integrity and availability of the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DB2 Recovery Expert for LUW - version 5.5 IF 2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7259901

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerabilities (CVE-2026-20129, CVE-2026-20127, CVE-2026-20128, CVE-2026-20122, CVE-2026-20133, CVE-2026-20126)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their Products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Manager deployed as: • On-Prem • Cisco Hosted SD-WAN Cloud • Cisco Hosted SD-WAN Cloud - Cisco Managed • Cisco Hosted SD-WAN Cloud - FedRAMP Environment
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v#details

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-31364)
Description	Dell has released security updates addressing a vulnerability that exists in their products. **CVE-2023-31364 -** Improper handling of direct memory writes in the input-output memory management unit could allow a malicious guest virtual machine (VM) to flood a host with writes, potentially causing a fatal machine check error resulting in denial of service. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	**Versions prior to 1.5.3** PowerEdge R6715 PowerEdge R7715 PowerEdge R6725 PowerEdge R7725 PowerEdge R7725xd PowerEdge M7725 PowerEdge XE7745 **Versions prior to 1.14.1** PowerEdge R6615 PowerEdge R7615 PowerEdge R6625 PowerEdge R7625 Dell XC Core XC7625 **Versions prior to 1.9.1** PowerEdge C6615 **Versions prior to 1.2.3** PowerEdge XE9685L **Versions prior to 2.21.1** PowerEdge R6515 PowerEdge R6525 PowerEdge R7515 PowerEdge R7525 PowerEdge C6525 Dell EMC XC Core XC7525 **Versions prior to 2.19.1** PowerEdge XE8545 **Versions prior to 1.27.0** PowerEdge R6415 PowerEdge R7415 PowerEdge R7425
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000432584/dsa-2026-075-security-update-for-dell-amd-based-poweredge-server-vulnerability

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3218, CVE-2026-3217, CVE-2026-3216, CVE-2026-3215, CVE-2026-3214, CVE-2026-3213, CVE-2026-3212, CVE-2026-3211, CVE-2026-3210)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in the third party components of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Material Icons module versions prior to 2.0.4 Theme Negotiation by Rules module versions prior to 1.2.1 Tagify module versions prior to 1.2.49 Anti-Spam by CleanTalk module versions prior to 9.7.0 Captcha module versions 2.0.0 through 2.0.10 and prior to 1.17.0 Islandora module versions prior to 2.17.5 Drupal Canvas module versions prior to 1.1.1 SAML SSO- Service Provider module versions prior to 3.1.3 Responsive Favicons module versions prior to 2.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-011 https://www.drupal.org/sa-contrib-2026-012 https://www.drupal.org/sa-contrib-2026-013 https://www.drupal.org/sa-contrib-2026-014 https://www.drupal.org/sa-contrib-2026-015 https://www.drupal.org/sa-contrib-2026-016 https://www.drupal.org/sa-contrib-2026-017 https://www.drupal.org/sa-contrib-2026-018 https://www.drupal.org/sa-contrib-2026-019

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50865, CVE-2023-53513, CVE-2023-53821, CVE-2023-53827, CVE-2025-38022, CVE-2025-38415, CVE-2025-38459, CVE-2025-39760, CVE-2025-39933, CVE-2025-40269, CVE-2025-40271, CVE-2025-40304, CVE-2025-40322, CVE-2025-68349, CVE-2022-50673, CVE-2023-53539, CVE-2023-53581, CVE-2023-53673, CVE-2023-53833, CVE-2026-23074)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the kernel component of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 • Red Hat Enterprise Linux Server - TUS 8.8 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 • Red Hat Enterprise Linux Server - AUS 8.4 x86_64 • Red Hat Enterprise Linux Server - AUS 8.2 x86_64 • 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 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:3360 https://access.redhat.com/errata/RHSA-2026:3277 https://access.redhat.com/errata/RHSA-2026:3293 https://access.redhat.com/errata/RHSA-2026:3388

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20775, CVE-2022-20818, CVE-2026-20051, CVE-2026-20048, CVE-2026-20033, CVE-2026-20010, CVE-2026-20036, CVE-2026-20037, CVE-2026-20091, CVE-2026-20099)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. 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-ucsciv-wGYtC78q • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsfxosxss-7skVE8Zv • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-afwae-mOgUfyLn • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-cmdinj-GvxLPeSB • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n3kn9k_aci_lldp_dos-NdgRrrA3 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cpdos-qLsv6pFD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dsnmp-cNN39Uh • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ether-dos-Kv8YNWZ4 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-priv-E6e8tEdF

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	DB2 Recovery Expert for LUW - version 5.5 IF 2 IBM WebSphere Application Server – Liberty - Versions 17.0.0.3 through 26.0.0.2 IBM WebSphere Application Server - versions 9.0 & 8.5 QRadar AI Assistant - versions 1.0.0 through 1.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7259901 https://www.ibm.com/support/pages/node/7261887 https://www.ibm.com/support/pages/node/7261794 https://www.ibm.com/support/pages/node/7261761

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.