Advisory Alert

Alert Number: AAA20260319 **Date:** March 19, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Drupal	**Medium**	Cross Site Request Forgery Vulnerability

Description

Affected Product	**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 affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Policy Manager for Secure Connect Gateway – Appliance - Versions prior to 5.32.00.18 PowerSwitch Z9664F-ON - Versions prior to 3.54.5.1-11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000441138/dsa-2026-120-security-update-for-dell-secure-connect-gateway-policy-manager-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000441046/dsa-2026-140-security-update-for-dell-networking-products-for-rsync-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1188, CVE-2022-46337, CVE-2025-48913)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-1188:** An API function that returns the textual names of supported processor features did not properly account for separators between entries. If the output buffer was incorrectly sized, failing to consider these separators when checking write safety could lead to a buffer overflow. **CVE-2022-46337:** In LDAP-authenticated Derby environments, this vulnerability can allow attackers to fill disk space by creating junk databases, execute malicious code with the server's privileges, and—if SQL authorization is not properly enforced—access, modify, or corrupt sensitive data and run database functions. **CVE-2025-48913:** If untrusted users are allowed to configure JMS for Apache CXF, previously they could use RMI or LDAP URLs, potentially leading to code execution capabilities. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar – Versions 7.5.0 - 7.5.0 UP14 IF05
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7266711

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53794 CVE-2023-53827 CVE-2025-21738 CVE-2025-38224 CVE-2025-38375 CVE-2025-68285 CVE-2025-71066 CVE-2026-23004 CVE-2026-23060 CVE-2026-23074 CVE-2026-23089 CVE-2026-23191 CVE-2026-23204)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in the kernel of their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.3 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260928-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-52999, CVE-2025-12543, CVE-2025-48913, CVE-2025-55163, CVE-2025-4949, CVE-2026-0603, CVE-2024-7254, CVE-2024-3884, CVE-2025-9784)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in the Red Hat JBoss Enterprise Application Platform. These vulnerabilities could be exploited by malicious users to compromise affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 ELS 7.4 for RHEL 7 x86_64 JBoss Enterprise Application Platform 7.4 ELS 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 ELS 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 7.4 ELS 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:4915 • https://access.redhat.com/errata/RHSA-2026:4916 • https://access.redhat.com/errata/RHSA-2026:4917 • https://access.redhat.com/errata/RHSA-2026:4924

Affected Product	**IBM**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in the QRadar SIEM Product. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar – Versions 7.5.0 - 7.5.0 UP14 IF05
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7266711

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Cross Site Request Forgery Vulnerability (CVE-2026-4393)
Description	Drupal has released a security update addressing a vulnerability that exists in their product. **CVE-2026-4393**: The module doesn't sufficiently protect its routes from cross-site request forgery (CSRF), allowing the logout route to be triggered without user interaction. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Automated Logout 8.x-1.x – Versions prior to 1.7.0 Automated Logout 2.x – Versions prior to 2.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-030

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.