Advisory Alert

Alert Number: AAA20261020 **Date:** October 20, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
F5	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Security Update

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat OpenShift AI
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:84734

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796, CVE-2025-66412, CVE-2026-22610, CVE-2026-32635, CVE-2026-50557, CVE-2026-54265, CVE-2026-27970, CVE-2026-52725, CVE-2026-54267, CVE-2026-41691, CVE-2025-13465, CVE-2026-2950, CVE-2026-4800, CVE-2025-47914, CVE-2025-58181, CVE-2026-39827, CVE-2026-39828, CVE-2026-39829, CVE-2026-39830, CVE-2026-39831, CVE-2026-39832, CVE-2026-39833, CVE-2026-39834, CVE-2026-39835, CVE-2026-42508, CVE-2026-46595, CVE-2026-46597, CVE-2026-46598, CVE-2025-66035, CVE-2026-50170, CVE-2026-50171, CVE-2026-54266, CVE-2026-54268, CVE-2025-65637)
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 OpenManage Enterprise versions prior to 4.8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000523220/dsa-2026-467-security-update-for-dell-openmanage-enterprise-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-63073, CVE-2026-53791, CVE-2026-13221, CVE-2026-32327, CVE-2026-63382, CVE-2026-63385, CVE-2026-8927)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Infrastructure: IBM Guardium Data Protection version 12.2.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7292835

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43450, CVE-2026-46149, CVE-2026-53062, CVE-2026-63802, CVE-2026-63920, CVE-2026-63922, CVE-2026-63924)
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 Platform & Enterprise Software: Red Hat Enterprise Linux 8: • 8.4: Advanced Update Support (AUS) (x86_64), Extended Life Cycle Long Life (x86_64) • 8.8: Extended Life Cycle Long Life (x86_64), Update Services (TUS) (x86_64), Update Services for SAP Solutions (ppc64le, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:84793 https://access.redhat.com/errata/RHSA-2026:84677

Vendor	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42011, CVE-2026-42013, CVE-2026-42012)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-42011:** A flaw was found in gnutls. This vulnerability occurs because permitted name constraints were incorrectly ignored when previous Certificate Authorities (CAs) only had excluded name constraints. A remote attacker could exploit this to bypass critical name constraint checks during certificate validation. This bypass could lead to the acceptance of invalid certificates, potentially enabling spoofing or man-in-the-middle attacks against affected systems. **CVE-2026-42013:** A flaw was found in gnutls. When validating certificates, an oversized Subject Alternative Name (SAN) could cause the validation process to incorrectly fall back to checking the Common Name (CN) field. This could allow a remote attacker to bypass proper certificate validation, potentially leading to spoofing or man-in-the-middle attacks. **CVE-2026-42012:** A flaw was found in gnutls. A remote attacker could exploit this vulnerability by presenting a specially crafted certificate that contains Uniform Resource Identifier (URI) or Service (SRV) Subject Alternative Names (SANs). This could cause the certificate validation process to incorrectly fall back to checking DNS hostnames against the Common Name (CN), potentially allowing the attacker to spoof legitimate services or intercept sensitive information. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5 Infrastructure: F5 Insight versions 1.0.0 – 1.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000163776 https://my.f5.com/manage/s/article/K000163778 https://my.f5.com/manage/s/article/K000163777

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53131, CVE-2026-63794, CVE-2026-63887, CVE-2026-68158)
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Infrastructure: • openSUSE Leap 15.5 • SUSE Linux Enterprise 12 SP5: High Performance Computing, Live Patching, Server, Server for SAP Applications • SUSE Linux Enterprise 15 SP5: High Performance Computing, Live Patching, Real Time, Server, Server for SAP Applications • SUSE Linux Enterprise Micro 5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264734-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264733-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264730-1/

Vendor	**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 the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Infrastructure: • AIX versions 7.2 and 7.3 • IBM Guardium Data Protection versions 12.1, 12.2, and 12.2.3 • IBM Guardium Data Protection - DataLake component version 12.2.3 • IBM QRadar Pulse App versions 1.0.0 – 2.2.17 • Use Case Manager App versions 1.0.0 – 4.2.0 • VIOS version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7292996 https://www.ibm.com/support/pages/node/7292835 https://www.ibm.com/support/pages/node/7293014 https://www.ibm.com/support/pages/node/7293040 https://www.ibm.com/support/pages/node/7292996 https://www.ibm.com/support/pages/node/7293039

Vendor	**Dell**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2026-81472)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2026-81472:** Dell iDRAC Service Module (iSM) for Windows, Linux, and for ESXi, versions prior to 6.1.1.0, contains an Improper Control of Generation of Code ('Code Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Infrastructure: iDRAC Service Module (ESXi, Linux, Windows): versions prior to 6.1.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000523111/dsa-2026-458-security-update-for-dell-idrac-service-module-vulnerability

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.