



Advisory Alert

Alert Number: AAA20261009 Date: October 9, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	Critical	Multiple Vulnerabilities
HPE	Critical	Authentication Bypass Vulnerability
IBM	Critical	Multiple Vulnerabilities
Cisco	Critical	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities
F5	High	Multiple Vulnerabilities
SUSE	High	Multiple Vulnerabilities
IBM	High, Medium	Multiple Vulnerabilities
Ubuntu	High, Medium, Low	Multiple Vulnerabilities

Description

Vendor	Red Hat
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-102273, CVE-2026-45820, CVE-2026-59893, CVE-2026-63374, CVE-2026-69243, CVE-2026-76218, CVE-2026-76219, CVE-2026-76220, CVE-2026-76221, CVE-2026-76222, CVE-2026-78676, CVE-2026-91990, CVE-2026-96760)
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 Ansible Automation Platform
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:79378

Vendor	HPE
Severity	Critical
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-79842)
Description	HPE has released a security update addressing a vulnerability that exists in their products. CVE-2026-79842: An authentication bypass vulnerability exists in HPE Intelligent Management Center (iMC) prior to v7.3 E0713 HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Intelligent Management Center (iMC) - Prior to v7.3 E0713
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05157en_us&docLocale=en_US

Vendor	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84272, CVE-2026-80381, CVE-2026-75875)
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 Guardium Data Protection versions 12.0, 12.1, 12.2, 12.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288832 https://www.ibm.com/support/pages/node/7291674 https://www.ibm.com/support/pages/node/7291674

Vendor	Cisco
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76463, CVE-2026-76464, CVE-2026-76467, CVE-2026-76468, CVE-2026-76469, CVE-2026-76470, CVE-2026-76472, CVE-2026-76471)
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 NX-OS Software (NX-API enabled): - Nexus 3000 Series Switches - Nexus 9000 Series Switches (Standalone NX-OS mode) - UCS 6300 Series Fabric Interconnects Meraki Platforms: - Meraki Campus Gateways - Meraki MG Cellular Gateways - Meraki MR Wireless Access Points - Meraki MS Series Switches - Meraki MV Smart Cameras - Meraki MX Security & SD-WAN Appliances
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-meraki-os-drbEX9GH https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-napi-rce-r2shwu2j

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-63209, CVE-2026-83663, CVE-2026-84445, CVE-2026-94637, CVE-2026-11822, CVE-2026-11824, CVE-2026-54369, CVE-2026-58014, CVE-2026-58015, CVE-2025-66418)
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 OpenShift distributed tracing - Red Hat OpenShift Container Platform 4.14 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 - Red Hat OpenShift Container Platform 4.16 (RHEL 9): aarch64, ppc64le, s390x, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:79368 https://access.redhat.com/errata/RHSA-2026:73866 https://access.redhat.com/errata/RHSA-2026:73851

Vendor	F5
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0994, CVE-2026-42009, CVE-2026-42010)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. CVE-2026-0994: A denial-of-service (DoS) vulnerability exists in google.protobuf.json_format.ParseDict() in Python, where the max_recursion_depth limit can be bypassed when parsing nested google.protobuf.Any messages. Due to missing recursion depth accounting inside the internal Any-handling logic, an attacker can supply deeply nested Any structures that bypass the intended recursion limit, eventually exhausting Python's recursion stack and causing a RecursionError. CVE-2026-42009: A flaw found in gnutls. A remote attacker could exploit an issue in the Datagram Transport Layer Security (DTLS) packet reordering logic. The comparator function, responsible for ordering DTLS packets by sequence numbers, did not correctly handle packets with duplicate sequence numbers. This could lead to unstable packet ordering or undefined behavior, resulting in a denial of service. CVE-2026-42010: A flaw found in gnutls. Servers configured with RSA-PSK (Rivest–Shamir–Adleman – Pre-Shared Key) wrongfully matched usernames containing a NUL character with truncated usernames. A remote attacker could exploit this by sending a specially crafted username, leading to an authentication bypass. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next CNF versions 2.2.0 – 2.2.1 BIG-IP Next for Kubernetes versions 2.2.0 – 2.2.1 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/K000163608 https://my.f5.com/manage/s/article/K000163593 https://my.f5.com/manage/s/article/K000163594

Vendor	SUSE
Severity	High
Affected Vulnerability	Multiple Vulnerabilities
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	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 (including ESPOS & LTSS), Live Patching, Real Time, Server (including LTSS), 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-20264595-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264586-1/

Vendor	IBM
Severity	High, Medium
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 Guardium Data Protection versions 12.0, 12.1, 12.2, and 12.2.2 IBM Db2 versions 11.5.0 – 11.5.9 and 12.1.0 – 12.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288832 https://www.ibm.com/support/pages/node/7288838 https://www.ibm.com/support/pages/node/7291674 https://www.ibm.com/support/pages/node/7291675 https://www.ibm.com/support/pages/node/7291670 https://www.ibm.com/support/pages/node/7291674 https://www.ibm.com/support/pages/node/7291606 https://www.ibm.com/support/pages/node/7291609 https://www.ibm.com/support/pages/node/7291607 https://www.ibm.com/support/pages/node/7291613 https://www.ibm.com/support/pages/node/7291612 https://www.ibm.com/support/pages/node/7291610

Vendor	Ubuntu
Severity	High, Medium, Low
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 22.04 and 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8906-1 https://ubuntu.com/security/notices/USN-8905-1 https://ubuntu.com/security/notices/USN-8904-1 https://ubuntu.com/security/notices/USN-8903-1 https://ubuntu.com/security/notices/USN-8888-2 https://ubuntu.com/security/notices/USN-8887-2

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.