TLP: WHITE

Advisory Alert

Alert Number: **AAA20260205** **Date:** **February 5, 2026**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Check Point	**High**	Directory Traversal Vulnerability
HPE	**High**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
cPanel	**Medium**	Multiple Vulnerabilities
Nginx	**Medium**	Proxy Man-in-the-Middle (MITM) Injection Vulnerability
F5	**Medium, Low**	Multiple Vulnerabilities
Drupal	**Low**	Access Bypass Vulnerability

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49290, CVE-2022-50341, CVE-2023-53751, CVE-2025-39971, CVE-2025-40154, CVE-2025-40248, CVE-2025-40277, CVE-2025-68301, CVE-2025-12183, CVE-2025-66566, CVE-2025-68285)
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 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 Server - AUS 8.4 x86_64 • JBoss Enterprise Application Platform Text-Only Advisories x86_64 • Red Hat Enterprise Linux for x86_64 9 x86_64 • Red Hat Enterprise Linux for Power, little endian 9 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:1886 https://access.redhat.com/errata/RHSA-2026:1872 https://access.redhat.com/errata/RHSA-2026:1820 https://access.redhat.com/errata/RHSA-2026:1935

Affected Product	**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 affected systems. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• openSUSE Leap 15.3 • SUSE Linux Enterprise Micro 5.2 • SUSE Linux Enterprise Micro for Rancher 5.2 • SUSE Linux Enterprise Server 11 SP4 • SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20260369-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20260385-1/

Affected Product	**Check Point**
Severity	**High**
Affected Vulnerability	Directory Traversal Vulnerability (CVE-2025-9142)
Description	Check Point has released security updates addressing a vulnerability that exists in their Harmony SASE products. **CVE-2025-9142**: A local user can trigger the Check Point Harmony SASE Windows client to write or delete files outside the intended certificate working directory (improper pathname limitation / directory traversal). Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Harmony SASE versions prior to 12.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk184557

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24519, CVE-2025-27713, CVE-2025-32732, CVE-2025-33000, CVE-2025-33001, CVE-2025-33002, CVE-2025-33003, CVE-2025-33004, CVE-2025-33005, CVE-2025-33006)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious entities to carry out Denial of Service (DoS), Disclosure of information and Escalation of Privilege attacks. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Affected component: Intel QuickAssist Technology driver for Microsoft Windows • HPE ProLiant Compute XD230 - Prior to v2.6.0 • HPE Alletra Storage Server 4210 - Prior to v2.6.0 • HPE ProLiant Compute DL320 Gen12 - Prior to v2.6.0 • HPE ProLiant Compute DL340 Gen12 - Prior to v2.6.0 • HPE ProLiant Compute DL360 Gen12 - Prior to v2.6.0 • HPE ProLiant Compute DL380 Gen12 - Prior to v2.6.0 • HPE ProLiant Compute DL380a Gen12 - Prior to v2.6.0 • HPE ProLiant Compute DL580 Gen12 - Prior to v2.6.0 • HPE ProLiant Compute ML350 Gen12 - Prior to v2.6.0 • HPE Synergy 480 Gen12 Compute Module - Prior to v2.6.0 • HPE Compute Edge Server e930t - Prior to v2.6.0 • HPE Compute Scale-up Server 3200 - Prior to v2.6.0 • HPE Alletra 4110 - Prior to v2.6.0 • HPE Alletra 4120 - Prior to v2.6.0 • HPE Alletra 4140 - Prior to v2.6.0 • HPE ProLiant DL110 Gen11 - Prior to v2.6.0 • HPE ProLiant DL320 Gen11 Server - Prior to v2.6.0 • HPE ProLiant DL360 Gen11 Server - Prior to v2.6.0 • HPE ProLiant DL380 Gen11 Server - Prior to v2.6.0 • HPE ProLiant DL380a Gen11 - Prior to v2.6.0 • HPE ProLiant DL560 Gen11 - Prior to v2.6.0 • HPE ProLiant ML110 Gen11 - Prior to v2.6.0 • HPE ProLiant ML350 Gen11 Server - Prior to v2.6.0 • HPE Synergy 480 Gen11 Compute Module - Prior to v2.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesb3p04984en_us&docLocale=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38561, CVE-2025-39698, CVE-2025-40019, CVE-2025-40214)
Description	Ubuntu 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. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 25.10, 24.04, 22.04, 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8015-1 • https://ubuntu.com/security/notices/USN-8014-1 • https://ubuntu.com/security/notices/USN-8013-1

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20119, CVE-2026-20098, CVE-2026-20056, CVE-2026-20111, CVE-2026-20123)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS), Arbitrary File Upload, and Open Redirect attacks. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco TelePresence Collaboration Endpoint (CE) Software Cisco RoomOS Software Cisco Meeting Management Cisco Secure Web Appliance Cisco Prime Infrastructure Cisco Evolved Programmable Network Manager
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tce-roomos-dos-9V9jrC2q • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cmm-file-up-kY47n8kK • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-archive-bypass-Scx2e8zF • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-xss-bYeVKCD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-pi-redirect-6sX82dN

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-36427, CVE-2025-36424, CVE-2022-23471, CVE-2023-25153, CVE-2023-25173)
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	IBM Db2 for Linux, UNIX and Windows Versions: 11.5.0 to 11.5.9 Versions: 12.1.0 to 12.1.3 IBM Db2 Data Management Console Version: 3.1.13 or lower IBM Db2 Data Management Console on CPD Version: 4.7.x or lower
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7257696 • https://www.ibm.com/support/pages/node/7257695 • https://www.ibm.com/support/pages/node/7259526 • https://www.ibm.com/support/pages/node/7257681

Affected Product	**cPanel**
Severity	**Medium**
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)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their EasyApache products. These vulnerabilities could be exploited by malicious users to compromise affected systems. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 v25.45
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Affected Product	**Nginx**
Severity	**Medium**
Affected Vulnerability	Proxy Man-in-the-Middle (MITM) Injection Vulnerability (CVE-2026-1642)
Description	Nginx has released security updates addressing a vulnerability that exists in their products. **CVE-2026-1642** - A vulnerability exists in NGINX OSS and NGINX Plus when configured to proxy to upstream Transport Layer Security (TLS) servers. An attacker with a man-in-the-middle (MITM) position on the upstream server side may be able to inject plain text data into the response from an upstream proxied server. Nginx advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• NGINX Plus — R32 - R36 P1 • NGINX Open Source — 1.3.0 - 1.29.4 • NGINX Ingress Controller — 5.0.0 - 5.3.2 • NGINX Ingress Controller — 4.0.0 - 4.0.1 • NGINX Ingress Controller — 3.4.0 - 3.7.2 • NGINX Gateway Fabric — 2.0.0 - 2.4.0 • NGINX Gateway Fabric — 1.2.0 - 1.6.2 • NGINX Instance Manager — 2.15.1 - 2.21.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000159824

Affected Product	**F5**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	F5 has released their quarterly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) 21.0.0 17.5.0 - 17.5.1 17.1.0 - 17.1.3 16.1.0 - 16.1.6 BIG-IP APM 21.0.0 17.5.0 - 17.5.1 17.1.0 - 17.1.3 16.1.0 - 16.1.6 APM Clients 7.2.5 - 7.2.6.1 BIG-IP Container Ingress Services for Kubernetes and OpenShift 2.0.0 - 2.20.1 1.0.0 - 1.14.0 BIG-IP Advanced WAF/ASM 17.1.0 - 17.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000159076

Affected Product	**Drupal**
Severity	**Low**
Affected Vulnerability	Access Bypass Vulnerability (CVE-2026-1917)
Description	Drupal has released security updates addressing a vulnerability that exists in their products. **CVE-2026-1917** – An Access bypass vulnerability that exists due to the Login Disable module failing to check for the required access key on the HTTP login route, allowing bypass of the intended login restriction control. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Login Disable versions prior to 2.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-008

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.