TLP: WHITE

Advisory Alert

Alert Number: AAA20260508 **Date:** May 8, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Ivanti	**High**	Multiple Vulnerabilities
Juniper Networks	**High**	Status of Copy Fail Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High,** Medium, Low	Multiple Vulnerabilities
PHP	**High,** Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-16885, CVE-2026-31402, CVE-2025-40240, CVE-2026-23191)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in the kernel 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 Server - Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension 6 i386 Red Hat Enterprise Linux Server - Extended Life Cycle Support Extension (for IBM z Systems) 6 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:14823 • https://access.redhat.com/errata/RHSA-2026:14925

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-5786, CVE-2026-5787, CVE-2026-5788, CVE-2026-6973, CVE-2026-7821)
Description	Ivanti has released a security update addressing multiple vulnerabilities that exists their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Endpoint Manager Mobile (EPMM) – Versions 12.8.0.0 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/May-2026-Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM-Multiple-CVEs?language=en_US

Affected Product	**Juniper Networks**
Severity	**High**
Affected Vulnerability	Status of Copy Fail Vulnerability (CVE-2026-31431)
Description	Juniper has released a security update addressing a vulnerability that exists their products. **CVE-2026-31431:** Copy Fail is a logic bug in the crypto module's authencesn cryptographic template. It lets an unprivileged local user trigger a deterministic, controlled 4-byte write into the page cache of any readable file on the system. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS Evolved (EVO) Session Smart Router Junos Space
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2026-05-Reference-Advisory-Status-of-Copy-Fail-vulnerability-on-Juniper-Products-CVE-2026-31431

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38375, CVE-2025-39977, CVE-2025-71066, CVE-2026-23004, CVE-2026-23204, CVE-2026-31431)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists 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 15.4, 15.5 & 15.6 SUSE Linux Enterprise High Performance Computing 15 SP4 & SP5 SUSE Linux Enterprise Live Patching 15-SP4, SP5 & SP6 SUSE Linux Enterprise Micro 5.3, 5.4 & 5.5 SUSE Linux Enterprise Real Time 15 SP4, SP5, SP6 SUSE Linux Enterprise Server 15 SP4, SP5 & SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP4, SP5 & SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20261735-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261736-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20261733-1/

Affected Product	**Ubuntu**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security update 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 these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu – Versions 20.04, 22.04, 24.04 & 25.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8179-4 • https://ubuntu.com/security/notices/USN-8243-1 • https://ubuntu.com/security/notices/USN-8244-1 • https://ubuntu.com/security/notices/USN-8245-1 • https://ubuntu.com/security/notices/USN-8254-1 • https://ubuntu.com/security/notices/USN-8255-1 • https://ubuntu.com/security/notices/USN-8258-1

Affected Product	**PHP**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6735, CVE-2026-7259, CVE-2025-14179, CVE-2026-6722, CVE-2026-7261, CVE-2026-7262, CVE-2026-7568, CVE-2026-7258, CVE-2026-7263, CVE-2026-6104, CVE-2026-42371)
Description	PHP has released security updates addressing multiple vulnerabilities that exists their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP Versions prior to: • 8.2.31 • 8.3.31 • 8.4.21 • 8.5.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.php.net/ChangeLog-8.php#8.3.31 • https://www.php.net/ChangeLog-8.php#8.4.21 • https://www.php.net/ChangeLog-8.php#8.5.6 • https://www.php.net/ChangeLog-8.php#8.2.31

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.