Advisory Alert

Alert Number: AAA20260818 **Date:** August 18, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**	Improper Access Control Vulnerability
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53264, CVE-2026-31641, CVE-2026-43038, CVE-2026-43329, CVE-2026-46244, CVE-2026-64530, CVE-2026-43125, CVE-2025-39902, CVE-2026-17523, CVE-2026-43206, CVE-2026-53016, CVE-2026-53136, CVE-2026-53329, CVE-2026-53374, CVE-2026-63879, CVE-2026-63884, CVE-2026-64219)
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 Enterprise Linux 8 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x Red Hat Enterprise Linux 8.10 (Extended Life Cycle): x86_64, aarch64, ppc64le, s390x Red Hat Enterprise Linux 9 Base: x86_64, ppc64le Red Hat Enterprise Linux 9.2 (Advanced Update Support, Update Services for SAP Solutions, Four Years of Updates, Extended Life Cycle): x86_64, aarch64, ppc64le, s390x Red Hat Enterprise Linux 9.8 (Extended Update Support, Update Services for SAP Solutions, Extended Life Cycle): x86_64, ppc64le Red Hat Enterprise Linux 10 Base: x86_64, ppc64le Red Hat Enterprise Linux 10.2 (Extended Update Support, Four Years of Support/Updates, Extended Life Cycle): x86_64, ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:54515 https://access.redhat.com/errata/RHSA-2026:55618 https://access.redhat.com/errata/RHSA-2026:55763 https://access.redhat.com/errata/RHSA-2026:55764 https://access.redhat.com/errata/RHSA-2026:55837

Vendor	**HPE**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-20898)
Description	HPE has released a security update addressing a vulnerability that exist in their products. **CVE-2026-20898:** Improper access control in the firmware for some in Alias Checking Trusted Module for some Intel(R) Xeon(R) processors may allow an escalation of privilege. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra Storage Server 4210: Prior to v1.80_05-29-2026 HPE ProLiant Compute DL110 Gen12: Prior to v1.50_07-24-2026 HPE ProLiant Compute (DL320, DL340, DL360, DL380, DL380a, DL580, ML350) Gen12 & XD230: Prior to v1.80_05-29-2026 HPE Synergy 480 Gen12 Compute Module: Prior to v1.80_05-29-2026
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05116en_us&docLocale=en_US

Vendor	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53359, CVE-2026-53228, CVE-2026-53225, CVE-2026-53215, CVE-2026-53212, CVE-2026-53176, CVE-2026-53086, CVE-2026-52989, CVE-2026-52924, CVE-2026-46331, CVE-2026-46266, CVE-2026-43499, CVE-2026-43378, CVE-2026-43198, CVE-2026-31705, CVE-2026-31448, CVE-2026-31414, CVE-2025-27558, CVE-2026-53260, CVE-2026-53247, CVE-2026-53246, CVE-2026-53224, CVE-2026-53221, CVE-2026-53216, CVE-2026-53186, CVE-2026-53175, CVE-2026-53151, CVE-2026-53131)
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 24.04 LTS & 20.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8629-2 https://ubuntu.com/security/notices/USN-8631-4

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.