Advisory Alert

Alert Number: AAA20260908 **Date:** September 8, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
ASUS	**High**	Authentication Bypass Vulnerability
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40149, CVE-2026-43114, CVE-2026-46056, CVE-2026-46099, CVE-2026-46145, CVE-2026-46155, CVE-2026-53006, CVE-2026-53016, CVE-2026-63886, CVE-2026-64304)
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 Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x • Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x • Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le • Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:64767

Vendor	**ASUS**
Severity	**High**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-19397)
Description	ASUS has released a security update addressing a vulnerability that exists in their products. **CVE-2026-19397:** Missing authentication for a critical function in ASUS Control Center Express Agent allows an unauthenticated nearby user to control the host via a direct connection to the agent when the host has an active login session. ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ASUS Control Center Express versions prior to 1.7.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

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 20.04, 22.04, 24.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8730-1 https://ubuntu.com/security/notices/USN-8729-1 https://ubuntu.com/security/notices/USN-8728-1 https://ubuntu.com/security/notices/USN-8727-1 https://ubuntu.com/security/notices/USN-8726-1

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.