Advisory Alert

Alert Number: AAA20260622 **Date:** June 22, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
ASUS	**High**	Validation Bypass Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46331, CVE-2026-31474, CVE-2026-31641, CVE-2026-31669, CVE-2026-31772, CVE-2026-31786, CVE-2026-31787, CVE-2026-43056, CVE-2026-43260, CVE-2026-43330, CVE-2026-46056, CVE-2026-46125, CVE-2026-46152, CVE-2026-46166, CVE-2026-46173, CVE-2026-31419, CVE-2026-31488, CVE-2026-43279, CVE-2026-46090, CVE-2026-46135, CVE-2026-46145)
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	RHEL 8.4 (EUS/AUS): x86_64 RHEL 8.6 (EUS/AUS): x86_64 RHEL 8.8 (EUS/TUS/SAP): x86_64, ppc64le RHEL 8.10 (Extended Life Cycle): x86_64, aarch64, ppc64le, s390x RHEL 8 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x RHEL 10 Base & CodeReady Builder: x86_64, aarch64, ppc64le, s390x RHEL 10.2 (EUS/4-Year/ELS/CodeReady EUS): x86_64, aarch64, ppc64le, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:27709 https://access.redhat.com/errata/RHSA-2026:27707 https://access.redhat.com/errata/RHSA-2026:27288 https://access.redhat.com/errata/RHSA-2026:27353 https://access.redhat.com/errata/RHSA-2026:27355 https://access.redhat.com/errata/RHSA-2026:27704

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31431, CVE-2026-43284, CVE-2026-43500, CVE-2026-46300)
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell APEX Cloud Platform for Red Hat OpenShift versions prior to 03.06.01.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000479129/dsa-2026-257-security-update-for-dell-apex-cloud-platform-for-red-hat-openshift-for-multiple-third-party-component-vulnerabilities

Vendor	**ASUS**
Severity	**High**
Affected Vulnerability	Validation Bypass Vulnerability (CVE-2026-8918)
Description	ASUS has released a security update addressing a vulnerability that exist in their products. **CVE-2026-8918:** A permissive list of allowed inputs in ASUS Armoury Crate allows a local administrator to perform arbitrary memory read/write operations or cause a system crash (BSOD) by bypassing the validation mechanism. ASUS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Armoury Crate
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exists 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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

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.