Advisory Alert

Alert Number: AAA20260717 **Date:** July 17, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
cPanel	**Critical**	Buffer Overflow Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
NetApp	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
cPanel	**Medium**	Multiple Vulnerabilities

Description

Vendor	**cPanel**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-42533)
Description	cPanel has released a security update addressing a vulnerability that exists in their products. **CVE-2026-42533:** Heap buffer overflow when using map with regex, potentially allowing remote code execution or worker process denial of service via a crafted HTTP request. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ea-nginx versions 0.9.6 to 1.31.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53016, CVE-2025-68183, CVE-2026-31408, CVE-2026-31613, CVE-2026-43027, CVE-2026-43499, CVE-2026-46189, CVE-2026-46209, CVE-2026-53166)
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 10 Red Hat Enterprise Linux - Extended Update Support 10.2 Red Hat Enterprise Linux - 4 years of updates 10.2 Red Hat Enterprise Linux - Extended Life Cycle 10.2 Red Hat CodeReady Linux Builder 10 Red Hat CodeReady Linux Builder - Extended Update Support 10.2 Red Hat Enterprise Linux - Extended Life Cycle Long Life 8.8 Red Hat Enterprise Linux Server - TUS 8.8 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:39494 https://access.redhat.com/errata/RHSA-2026:40760

Vendor	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42511, CVE-2026-0990)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-42511:** All supported versions of FreeBSD are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, Denial of Service (DoS). **CVE-2026-0990:** Multiple NetApp products incorporate libxml2. Libxml2 versions through 2.15.1 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 NetApp Manageability SDK
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20260501-0005 https://security.netapp.com/advisory/ntap-20260220-0013

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-50645, CVE-2026-9322, CVE-2026-9171, CVE-2026-11541, CVE-2026-9320, CVE-2026-8646, CVE-2026-11806, CVE-2026-9071, CVE-2026-11546, CVE-2026-5516, CVE-2026-4410, CVE-2026-11714, CVE-2026-14971)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PowerVM Novalink Versions: • 2.2.0, 2.2.1 and 2.2.1.1 • 2.3.0, 2.3.0.1, 2.3.1 and 2.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7280226 https://www.ibm.com/support/pages/node/7280225

Vendor	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-60005, CVE-2026-56434)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-60005:** Memory disclosure when using ngx_http_slice_module. **CVE-2026-56434:** Use-after-free when using ngx_http_ssi_module. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ea-nginx versions 0.8.11 to 1.31.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

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.