Advisory Alert

Alert Number: AAA20260708 **Date:** July 8, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Cross Site Scripting Vulnerabilities
Check Point	**High**	Improper Authentication Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Joomla	**Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Cross Site Scripting Vulnerabilities (CVE-2026-11712, CVE-2026-11708)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-11712:** IBM WebSphere Application Server 9.0, and 8.5 is affected by a cross-site scripting vulnerability in the administrative console help system. **CVE-2026-11708:** IBM WebSphere Application Server 9.0, and 8.5 is affected by a cross-site scripting vulnerability in the administrative console's integrated help system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak for Applications versions 5.1, 5.2 and 5.3 IBM WebSphere Application Server versions: • 9.0.0.0 - 9.0.5.28 • 8.5.5.0 - 8.5.5.29
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7279321

Vendor	**Check Point**
Severity	**High**
Affected Vulnerability	Improper Authentication Vulnerability (CVE-2026-50751)
Description	Check Point has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-50751:** An attacker can bypass user authentication by exploiting a logic flow weakness in the Remote Access and Mobile Access certificate validation and establish a remote access VPN connection without a valid user password. Check Point is aware of this vulnerability being exploited in the wild. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Security Gateways: • R82.10 Jumbo Hotfix Take 19 or below • R82 Jumbo Hotfix Take 103 or below • R81.20 Jumbo Hotfix Take 141 or below • R81.10 (EOS) • R81 (EOS) • R80.40 (EOS) Spark Firewalls: R80.20.X (EOS), R81.10.X, R82.00.X
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk185033

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23401, CVE-2026-31402, CVE-2026-31419, CVE-2026-43112, CVE-2026-42055, CVE-2026-43198, CVE-2026-43450, CVE-2026-46227, CVE-2026-46209, CVE-2026-46259, CVE-2025-10263, CVE-2025-12799, CVE-2026-46181, CVE-2025-68183, CVE-2026-31408, CVE-2026-46189, CVE-2026-46135)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:36534 • https://access.redhat.com/errata/RHSA-2026:36366 • https://access.redhat.com/errata/RHSA-2026:36364 • https://access.redhat.com/errata/RHSA-2026:36349 • https://access.redhat.com/errata/RHSA-2026:36345 • https://access.redhat.com/errata/RHSA-2026:36343 • https://access.redhat.com/errata/RHSA-2026:36342 • https://access.redhat.com/errata/RHSA-2026:36216 • https://access.redhat.com/errata/RHSA-2026:36073

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44877, CVE-2026-40912, CVE-2026-39806, CVE-2026-39803, CVE-2026-31431)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• HPE Networking Instant On 1830, 1930, and 1960 switches running software versions 3.3.3 and below • HPE Aruba Networking Private 5G Core 1.26.1.0 and below. • HPE Aruba Networking Management Software (Airwave) 8.3.0.6 and below. • HPE Aruba Networking AOS-CX: • AOS-CX 10.17.xxxx: AOS-CX 10.17.1010 and below • AOS-CX 10.16.xxxx: AOS-CX 10.16.1040 and below • AOS-CX 10.13.xxxx: AOS-CX 10.13.1170 and below • HPE Aruba Networking EdgeConnect Orchestrator all supported versions. • HPE Aruba Networking Analytics and Location Engine (ALE) all supported versions. • HPE Aruba Networking Meridian Asset Tracking
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05038en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05077en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05059en_us&docLocale=en_US

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-11595, CVE-2026-11546, CVE-2026-11714, CVE-2026-11806)
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	IBM Cloud Pak for Applications versions 5.1, 5.2 and 5.3 IBM WebSphere Application Server versions 9.0.0.0 - 9.0.5.28 and 8.5.5.0 - 8.5.5.29 IBM WebSphere Application Server Liberty 17.0.0.3 - 26.0.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7279321 • https://www.ibm.com/support/pages/node/7279273 • https://www.ibm.com/support/pages/node/7279278 • https://www.ibm.com/support/pages/node/7279277

Vendor	**Joomla**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48958, CVE-2026-48957, CVE-2026-48956, CVE-2026-48955, CVE-2026-48954, CVE-2026-48953, CVE-2026-48952, CVE-2026-48951, CVE-2026-48950, CVE-2026-48949, CVE-2026-48948, CVE-2026-48947)
Description	Joomla 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. Joomla advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Joomla! CMS versions 3.0.0-5.4.6 and 6.0.0-6.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

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.