Advisory Alert

Alert Number: AAA20261112 **Date:** November 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Information Disclosure Vulnerability
Apache HTTP Server	**Critical**	Race Condition Vulnerability
Check Point	**High**	Use-After-Free Vulnerability
Red Hat	**High, Medium**	Multiple Vulnerabilities
cPanel	**High, Medium, Low**	Multiple Vulnerabilities
IBM	**High, Medium, Low**	Multiple Vulnerabilities
NodeJS	**High, Medium, Low**	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities
F5	**Medium**	Race Condition Vulnerability
Palo Alto Networks	**Medium, Low**	Multiple Vulnerabilities
Apache HTTP Server	**Medium, Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-103111, CVE-2026-111497, CVE-2026-114406, CVE-2026-34182, CVE-2026-43114, CVE-2026-45445, CVE-2026-59995, CVE-2026-59999, CVE-2026-60002, CVE-2026-64564, CVE-2026-68121, CVE-2026-80792, CVE-2026-80863, CVE-2026-80864, CVE-2026-86145, CVE-2026-89161, CVE-2026-98432, CVE-2026-99999, CVE-2025-47273, CVE-2026-16313, CVE-2026-28390, CVE-2026-42011, CVE-2026-42013, CVE-2026-45447, CVE-2026-55653, CVE-2026-86138, CVE-2026-86140, CVE-2026-86142, CVE-2026-86143, CVE-2026-86144, CVE-2026-89846, CVE-2026-111943, CVE-2026-25681, CVE-2026-33814, CVE-2026-39821, CVE-2026-92092)
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 OpenShift Container Platform 4.15 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.15 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.15 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.15 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.15 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.15 for RHEL 8 aarch64 Red Hat OpenShift Container Platform 4.13 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.13 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.13 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.13 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.13 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.13 for RHEL 8 aarch64 Red Hat OpenShift Container Platform 4.17 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.17 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.17 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.17 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.17 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.17 for RHEL 8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:96282 • https://access.redhat.com/errata/RHSA-2026:95745 • https://access.redhat.com/errata/RHSA-2026:95754 • https://access.redhat.com/errata/RHSA-2026:95755

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2026-13697)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-13697:** undici's cache interceptor mishandles malformed Cache-Control private directives. In undici 7.0.0 up to before 7.29.0 and 8.0.0 up to before 8.9.0, a response carrying a degenerate qualified private directive, such as private set to an empty value, can be stored in the default shared cache and later served to a different caller with the same cache key, disclosing private response bodies and headers including Set-Cookie. Separately, a Cache-Control header that combines an unqualified private directive with a qualified one triggers an uncaught TypeError in the cache-control parser, which rejects the request and, depending on the consumer's error handling, can terminate the process. Both issues affect applications using the cache interceptor in shared mode, including the default configuration. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security QRadar EDR Versions - 3.12 - 3.12.26
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7296321

Vendor	**Apache HTTP Server**
Severity	**Critical**
Affected Vulnerability	Race Condition Vulnerability (CVE-2026-119618)
Description	Apache HTTP Server has released a security update addressing a vulnerability that exists in their products. **CVE-2026-119618:** Concurrent Execution using Shared Resource with Improper Synchronization vulnerability in Apache HTTP Server's mod_http2 in assign_headers() can lead to RCE. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.70. Affected releases of mod_h2 from GitHub: from 2.0.8 through 2.0.42. Apache HTTP Server advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HTTP Server: from 2.4.55 through 2.4.70.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Vendor	**Check Point**
Severity	**High**
Affected Vulnerability	Use-After-Free Vulnerability (CVE-2026-98432)
Description	Check Point has released a security update addressing a vulnerability that exists in their products. **CVE-2026-98432:** A use-after-free in the Linux kernel’s IPv4 TCP code. In tcp_v4_syn_recv_sock(), the child socket takes over ireq->ireq_opt without copying it. If another CPU is processing a retransmitted SYN for the same request socket, it can still be reading those options (tcp_v4_send_synack(), ip_options_build()) after the child socket is freed. The same race exists with request socket migration (tcp_migrate_req=1 or a BPF reuseport migrate program). inet_sock_destruct() and tcp_v4_reqsk_destructor() free the options with a plain kfree(), so the readers can touch freed memory. The fix switches both to kfree_rcu(), which delays freeing until RCU readers are done. IPv6 isn’t affected by the first issue, and a separate patch will handle the IPv6 migration case. Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• R82.20, R82.10, R82 • Spark Firewalls R81.10.x, R82.00.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk1000339

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
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 Platform & Enterprise Software: • Red Hat OpenShift Container Platform 4.17 (RHEL 8, RHEL 9): x86_64, ppc64le, s390x, aarch64 • Red Hat OpenShift Container Platform 4.13 (RHEL 8, RHEL 9): x86_64, ppc64le, s390x, aarch64 • Red Hat OpenShift Security Profiles Operator • JBoss Enterprise Application Platform 8.1 (RHEL 8, RHEL 9, RHEL 10): x86_64 • JBoss Enterprise Application Platform 7.4 ELS (RHEL 7, RHEL 8, RHEL 9): x86_64 • JBoss Enterprise Application Platform Text-Only Advisories: x86_64 Red Hat Enterprise Linux 10: • Base & CRB 10: aarch64, ppc64le, s390x, x86_64 • 10.2: Extended Update Support (all archs), 4 Years of Updates (aarch64, s390x, x86_64), 4 Years of Support (ppc64le), Extended Life Cycle (all archs); CRB EUS (all archs) Red Hat Enterprise Linux 9: • Base & CRB 9: aarch64, ppc64le, s390x, x86_64 • 9.4: Advanced Update Support (x86_64), Extended Life Cycle (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, x86_64) • 9.6: Extended Update Support (all archs), Advanced Update Support (x86_64), 4 Years of Updates (aarch64, s390x), Extended Life Cycle (all archs), Update Services for SAP Solutions (ppc64le, x86_64); CRB EUS (all archs) • 9.8: Extended Update Support (all archs), 4 Years of Updates (aarch64, s390x), Extended Life Cycle (all archs), Update Services for SAP Solutions (ppc64le, x86_64); CRB EUS (all archs) Red Hat Enterprise Linux 8: • Base & CRB 8: aarch64, ppc64le, s390x, x86_64 • 8.10: Extended Life Cycle (all archs) • Red Hat Enterprise Linux 6: • Extended Life Cycle Support Extension: x86_64, i386, s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/security-updates/

Vendor	**cPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-123863, CVE-2026-123864, CVE-2026-123865, CVE-2026-123866, CVE-2026-123872, CVE-2026-123874, CVE-2026-123828, CVE-2026-123867, CVE-2026-123868, CVE-2026-123871, CVE-2026-123875, CVE-2026-123877, CVE-2026-123829, CVE-2026-123862, CVE-2026-123873, CVE-2026-106071)
Description	cPanel 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. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	EasyApache: • ea-apache24 • ea-apr-util • ea-nghttp2 • ea-nodejs22 • ea-php82 • ea-php83 • ea-php84 • ea-php85
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-80179, CVE-2026-69185, CVE-2026-59879, CVE-2026-59880, CVE-2026-44722, CVE-2026-44432, CVE-2026-69247, CVE-2026-69248, CVE-2026-69249, CVE-2026-54272, CVE-2026-54282, CVE-2026-54283, CVE-2026-14643, CVE-2026-15157, CVE-2026-16728, CVE-2026-16729, CVE-2026-77037, CVE-2026-77063, CVE-2026-77078, CVE-2026-82333, CVE-2026-18401)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Security QRadar EDR Versions - 3.12 - 3.12.26
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7296321

Vendor	**NodeJS**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-123863, CVE-2026-123864, CVE-2026-123865, CVE-2026-123866, CVE-2026-126051, CVE-2026-123872, CVE-2026-123874, CVE-2026-123828, CVE-2026-123867, CVE-2026-123868, CVE-2026-123871, CVE-2026-123877, CVE-2026-123875, CVE-2026-123829, CVE-2026-123862, CVE-2026-106071)
Description	NodeJS 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. NodeJS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Node.js versions 26.x, 24.x, and 22.x.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/november-2026-security-releases

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-126744, CVE-2026-126728, CVE-2026-126727)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-126744:** The module provides its own Ajax command to open the iframe dialog. This command does not sanitize the dialog options the same way Drupal core does since SA-CORE-2026-001, which can lead to a cross-site scripting (XSS) vulnerability. **CVE-2026-126728:** The module does not sufficiently protect an action to restore a duplicate translation. A crafted request can cause a user with access to the translation overview to overwrite an existing translation and delete the duplicate, even if that user cannot edit or delete translations. **CVE-2026-126727:** The module does not sufficiently validate translation HTML and can display stored translations without sufficient filtering. A user who can create or edit string translations could inject JavaScript into pages that render those translations. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal Modules: • Texts: key-based strings and translations Versions - <1.0.17 • Layout Builder iFrame Modal Versions - <1.3.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2026-335 • https://www.drupal.org/sa-contrib-2026-319 • https://www.drupal.org/sa-contrib-2026-318

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	Race Condition Vulnerability (CVE-2026-46086)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2026-46086:** A race condition in the Linux kernel's bridge FDB code lets fdb_delete_local() change f->dst to another port or NULL while RCU readers such as br_fdb_fillbuf() (via the brforward_read() sysfs path) are still using it. Because the readers load f->dst more than once, a concurrent update between the NULL check and the port_no dereference can cause a NULL pointer dereference. The fix takes a single READ_ONCE() snapshot of f->dst in each affected reader and publishes the writer's updates with WRITE_ONCE(). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• F5 Insight Versions - 1.0.0 - 1.2.2 • F5OS Versions - 2.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000164202

Vendor	**Palo Alto Networks**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0331, CVE-2026-0330, CVE-2026-0329, CVE-2026-0328, CVE-2026-0327, CVE-2026-0326, CVE-2026-0325, CVE-2026-0324, CVE-2026-0323)
Description	Palo Alto Networks 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. Palo Alto Networks 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://security.paloaltonetworks.com/CVE-2026-0331 • https://security.paloaltonetworks.com/CVE-2026-0330 • https://security.paloaltonetworks.com/CVE-2026-0329 • https://security.paloaltonetworks.com/CVE-2026-0328 • https://security.paloaltonetworks.com/CVE-2026-0327 • https://security.paloaltonetworks.com/CVE-2026-0326 • https://security.paloaltonetworks.com/CVE-2026-0325 • https://security.paloaltonetworks.com/CVE-2026-0324 • https://security.paloaltonetworks.com/CVE-2026-0323

Vendor	**Apache HTTP Server**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-106023, CVE-2026-109163)
Description	Apache HTTP Server has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-106023:** NULL pointer dereference vulnerability in Apache HTTP Server's mod_md during HTTP request processing. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.69. **CVE-2026-109163:** Stack-based buffer overflow vulnerability in Apache HTTP Server's mod_vhost_alias (after CVE-2026-63292) This issue affects Apache HTTP Server: 2.4.69. Apache HTTP Server advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache HTTP Server Versions: • 2.4.30 through 2.4.70 • 2.4.69 and 2.4.70
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

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.