Advisory Alert

Alert Number: AAA20261027 **Date:** October 27, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
PHP	**Critical**	Buffer Overflow Vulnerability
Palo Alto Networks	**Critical**	Buffer Overflow Vulnerability
IBM	**Critical**	XML External Entity (XXE) Injection Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
F5	**Medium**	Relative Path Traversal Vulnerability
ASUS	**Medium**	Improper Access Control Vulnerability

Description

Vendor	**PHP**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-111497)
Description	PHP has released a security update addressing a vulnerability that exists in their products. **CVE-2026-111497:** vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream. PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Brotli versions 1.0.3 through 1.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/archive/2026.php#2026-10-26-1

Vendor	**Palo Alto Networks**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-111497)
Description	Palo Alto Networks has released a security update addressing a vulnerability that exists in their products. **CVE-2026-111497:** vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Palo Alto Networks Infrastructure: PAN-OS: • 11.2: prior to 11.2.4-h23, 11.2.7-h23, 11.2.10-h17, 11.2.13-h4, 11.2.16-h1 • 12.1: prior to 12.1.4-h13, 12.1.7-h11, 12.1.10-h3 • 12.2: prior to 12.2.4-h1 Prisma Cloud: Application Security Transporter Client: prior to 0.2.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-111497

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	XML External Entity (XXE) Injection Vulnerability (CVE-2026-49875)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-49875:** Apache CXF's EndpointReferenceUtils and W3CMultiSchemaFactory classes construct a SAXParserFactory without the necessary JAXP hardening configurations, enabling out-of-band (OOB) external entity resolution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Infrastructure: PowerVM NovaLink: 2.2.0, 2.2.1, 2.2.1.1, 2.3.0, 2.3.0.1, 2.3.1, 2.3.2 and 2.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7294118

Vendor	**Red Hat**
Severity	**High**
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 Dev Spaces Red Hat OpenShift Container Platform 4.21 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat Enterprise Linux 8: Base & CRB 8: aarch64, ppc64le, s390x, x86_64 8.10: Extended Life Cycle (all archs) Red Hat Enterprise Linux 9: 9.6: Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), Extended Update Support (EUS) & CodeReady Linux Builder EUS (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:89816 https://access.redhat.com/errata/RHSA-2026:89890 https://access.redhat.com/errata/RHSA-2026:90314 https://access.redhat.com/errata/RHSA-2026:90321 https://access.redhat.com/errata/RHSA-2026:89229

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-59280, CVE-2026-19032, CVE-2026-86472, CVE-2026-84394, CVE-2026-84292, CVE-2026-91777, CVE-2026-91776, CVE-2026-101909, CVE-2026-101908, CVE-2026-101907, CVE-2026-101906, CVE-2026-101905, CVE-2026-101904, CVE-2026-101903, CVE-2026-101902, CVE-2026-101901, CVE-2026-101900, CVE-2026-101898, CVE-2026-93749, CVE-2026-114406, CVE-2026-66144, CVE-2026-66143, CVE-2026-66142, CVE-2026-65432, CVE-2026-11713, CVE-2026-77816, CVE-2026-79715, CVE-2026-14909, CVE-2026-14532)
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 Infrastructure: • IBM Db2 Developer Extension: 1.1.2 • IBM QRadar Hub: 1.0.0 – 3.9.1 • IBM QRadar SIEM: 7.5.0 – 7.5.0 UP16 IF02, 7.6.0.0 – 7.6.0.5 • PowerVM NovaLink: 2.2.0, 2.2.1, 2.2.1.1, 2.3.0, 2.3.0.1, 2.3.1, 2.3.2, 2.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7294153 https://www.ibm.com/support/pages/node/7294154 https://www.ibm.com/support/pages/node/7294156 https://www.ibm.com/support/pages/node/7294158 https://www.ibm.com/support/pages/node/7294172 https://www.ibm.com/support/pages/node/7294092 https://www.ibm.com/support/pages/node/7294118

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	Relative Path Traversal Vulnerability (CVE-2026-59995)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2026-59995:** sftp in OpenSSH before 10.4 does not properly constrain the location of downloaded files when "sftp server:/path ." is used with an attacker-controlled server. This vulnerability allows a remote attacker-controlled server to cause a partial denial of availability and allows limited ability to modify data. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5 Infrastructure: • BIG-IP Next CNF: 2.2.0 – 2.2.3 and 2.3.0 – 2.3.2 • BIG-IP Next for Kubernetes: 2.2.0 – 2.2.3 and 2.3.0 – 2.3.2 F5OS: 2.0.0 F5OS-A: 1.5.1 – 1.5.4 and 1.8.0 – 1.8.4 F5OS-C: 1.8.0 – 1.8.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000163738

Vendor	**ASUS**
Severity	**Medium**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-88781)
Description	ASUS has released a security update addressing a vulnerability that exists in their products. **CVE-2026-88781:** This update addresses a security vulnerability related to improper access control in certain ASUS motherboard BIOS. If exploited, the issue could allow a local attacker with elevated privileges to affect system stability or data integrity. ASUS advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Motherboard BIOS Infrastructure: A520/B550 Series: prior to 3644/4304 X570 Series: prior to 5054 A620/A620A Series: prior to 4003/4004 B650 Series: prior to 1303/4003/4004 X670 Series: prior to 4003/4004 B840 Series: prior to 1804 B850 Series: prior to 1103/1804/2503 X870 Series: prior to 1804/2503 X870E Series: prior to 1103/2503 Knoll Series: prior to 4003 TRX50 Series: prior to 0703/1403 W790 Series: prior to 2101 WRX90 Series: prior to 1403
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

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.