Advisory Alert

Alert Number: AAA20261026 **Date:** October 26, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
QNAP	Critical	Multiple Vulnerabilities
IBM	Critical	Multiple Vulnerabilities
HPE	Critical	Multiple Vulnerabilities
Dell	Critical	Multiple Vulnerabilities
Oracle	Critical	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities
HP	High	Multiple Vulnerabilities
SUSE	High	Multiple Vulnerabilities
MongoDB	High, Medium	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities
Citrix	Medium	Improper Certificate Validation Vulnerability

Description

Vendor	**QNAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	QNAP has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** Memory corruption during out-of-memory (OOM) handling. A crafted HTTP request can exhaust memory while request data is only partly initialized, causing PHP cleanup to process invalid data. **CVE-2026-109619:** Use-after-free from stale global state retained between requests. A later request handled by the same PHP worker can access memory freed by an earlier request, leading to code execution or memory disclosure. QNAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• QTS 6.1.0 • QTS 5.2.11 and earlier • QuTS hero h6.1.0 • QuTS hero h6.0.x • QuTS hero h5.2.11 and earlier • QuTScloud c5.2.9 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-26-18

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-96760, CVE-2026-104056, CVE-2026-85394)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-96760:** Authlib (v1.7.2 and below) contains a signature verification bypass vulnerability. The JsonWebSignature.deserialize_json() method accepts a JSON Serialization JWS object and returns the payload as successfully verified without checking for a signature and without requiring a cryptographic key. **CVE-2026-104056:** Authlib version 1.7.2 and below contains a vulnerability where discovery JSON metadata is cached without validation or issuer-origin binding. This allows a poisoned discovery response to replace all endpoint values with attacker-controlled values rather than endpoint URLs that share the origin of the configured server metadata URL. **CVE-2026-85394:** python-jose through 3.5.0 fails to properly validate asymmetric keys in HMAC initialization, accepting DER-encoded public keys that lack PEM armor or SSH prefixes. Attackers holding the service's public key can forge HS256 tokens that pass verification when algorithms are not explicitly restricted. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Bridge Versions • 1.1.5.2 • 1.1.5.1 • 1.1.5.0 • 1.1.4.1 • 1.1.4.0 • 1.1.3.0 • 1.1.2.1 • 1.1.2.0 • 1.1.1.1 • 1.1.1.0 • 1.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7293989

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Aruba ClearPass Policy Manager Versions - 6.11.0, 6.11.4, 6.12.0, 6.11.5, 6.11.6, 6.11.7, 6.12.1, 6.11.8, 6.12.2, 6.11.9, 6.12.3, 6.11.10, 6.12.4, 6.11.11, 6.12.5, 6.11.12, 6.12.6, 6.11.13, 6.12.7, 6.14.0, 6.11.14, 6.12.8 • HPE Data Management Framework 7 DMF_Suite_4.10-rhel810 • HPE Private Cloud AI Versions - v1.11.0, 1.12.1, 2026.07.01 • Cray ClusterStor Data Services Versions -7.2, 7.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn05174en_us&docLocale=en_US

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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	Versions Prior to 6.2.0.0 for Vapp and Windows/Linux • Dell Storage Resource Manager • Dell Storage Monitoring and Reporting
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000524713/dsa-2026-462-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Vendor	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	Oracle has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Oracle Communications Diameter Signaling Router: 8.6.0, 9.0.0 Oracle Communications EAGLE Application Processor: 17.0, 17.1 Oracle Communications EAGLE Element Management System: 47.0 Oracle Communications EAGLE LNP Application Processor: 11.1 Oracle Communications LSMS: 14.0 Oracle Communications Performance Intelligence Center (PIC) Software: 10.4, 10.5 Oracle Communications Unified Assurance: 6.1.1-7.0.0 Oracle Communications User Data Repository: 15.0 Oracle Solaris: 11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/alert-cve-2026-109618.html

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-68745, CVE-2026-23199, CVE-2026-52972, CVE-2026-63831, CVE-2026-64061, CVE-2026-64319, CVE-2026-68200, CVE-2026-72243, CVE-2026-74641, CVE-2026-89846, CVE-2026-53236, CVE-2026-53388, CVE-2026-64378, CVE-2026-68136, CVE-2026-68338, CVE-2026-68140, CVE-2026-68138, CVE-2026-68476, CVE-2026-80586, CVE-2026-80824, CVE-2026-89638, CVE-2026-81003, CVE-2026-99999)
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 for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:89083 https://access.redhat.com/errata/RHSA-2026:88687

Vendor	**HP**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	HP has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). HP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HP Device Manager versions prior to 5.0.18.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hp.com/us-en/document/ish_15893017-15893060-16/hpsbhf04160

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53131, CVE-2026-63795, CVE-2026-63887, CVE-2026-63939, CVE-2026-68158, CVE-2026-63794)
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264889-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264888-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264887-1/

Vendor	**MongoDB**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-115929, CVE-2026-114655, CVE-2026-114654, CVE-2026-114653, CVE-2026-114652, CVE-2026-114651, CVE-2026-114650, CVE-2026-114649, CVE-2026-114648, CVE-2026-114647, CVE-2026-114646, CVE-2026-114645, CVE-2026-114644, CVE-2026-114643)
Description	MongoDB 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. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Compass Versions - affects versions prior to 1.53.1 libmongocrypt Versions - 1.0.0 affects versions prior to 1.21.1 C# Driver Versions: • 1.8.0 affects versions prior to 3.13.0 • 2.0.0 affects versions prior to 3.13.0 • 2.10.0 affects versions prior to 3.13.0 • 2.13.0 affects versions prior to 3.13.0 • 2.14.0 affects versions prior to 3.13.0 • 2.26.0 affects versions prior to 3.13.0 • 3.5.0 affects versions prior to 3.13.0 C Driver Versions: • 1.6.0 affects versions prior to 1.30.14 • 2.0.0 affects versions prior to 2.5.7 MongoDB.Libmongocrypt NuGet package Versions - 1.0.0 affects 1.12.0 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-97687, CVE-2026-97688, CVE-2026-97689, CVE-2026-19032, CVE-2026-68497, CVE-2026-83557, CVE-2026-91776, CVE-2026-91777, CVE-2026-93749, CVE-2026-101898, CVE-2026-101900, CVE-2026-101901, CVE-2026-101902, CVE-2026-101903, CVE-2026-101904, CVE-2026-101905, CVE-2026-101906, CVE-2026-101907, CVE-2026-101908, CVE-2026-101909)
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 Db2 Bridge Versions • 1.1.5.2 • 1.1.5.1 • 1.1.5.0 • 1.1.4.1 • 1.1.4.0 • 1.1.3.0 • 1.1.2.1 • 1.1.2.0 • 1.1.1.1 • 1.1.1.0 • 1.1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7293989

Vendor	**Citrix**
Severity	**Medium**
Affected Vulnerability	Improper Certificate Validation Vulnerability (CVE-2026-114406)
Description	Citrix has released a security update addressing a vulnerability that exists in their products. **CVE-2026-114406:** XenServer's internal list of trusted certificate authorities (CAs) included a public CA whose intermediate certificates have been found to have weak keys. This would allow a malicious attacker on the management network to forge TLS certificates that appeared to be signed by that trusted CA and so appear to a XenServer host to be a trusted LDAPS server, potentially authorising attacker access. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	XenServer 8.4 and XenServer 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697257&articleURL=XenServer_Security_Update_for_CVE_2026_114406

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.