Advisory Alert

Alert Number: AAA20260318 **Date:** March 18, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Security Update
Citrix	**High**	Privilege Escalation Vulnerability
MongoDB	**High**	Multiple Vulnerabilities
IBM	**High**, Low	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-55752, CVE-2025-55754, CVE-2025-61795)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in the Apache Tomcat component utilized by their NetWorker product. **CVE-2025-55752**: For rewrite rules that rewrite query parameters to the URL, an attacker could manipulate the request URI to bypass security constraints including the protection for /WEB-INF/ and /META-INF/. If PUT requests were also enabled then malicious files could be uploaded leading to remote code execution. **CVE-2025-55754**: If Tomcat was running in a console on a Windows operating system, and the console supported ANSI escape sequences, it was possible for an attacker to use a specially crafted URL to inject ANSI escape sequences to manipulate the console and the clipboard and attempt to trick an administrator into running an attacker controlled command. **CVE-2025-61795**: If an error occurred (including exceeding limits) during the processing of a multipart upload, temporary copies of the uploaded parts written to disc were not cleaned up immediately but left for the garbage collection process to delete. Depending on JVM settings, application memory usage and application load, it was possible that space for the temporary copies of uploaded parts would be filled faster than GC cleared it, leading to a DoS. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetWorker Management Web UI (NWUI) Versions 19.9 through 19.13.0.2 and 19.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000440823/dsa-2026-057-security-update-for-dell-networker-apache-tomcat-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2026-1002)
Description	Red Hat has released a security update addressing a vulnerability that exists in Red Hat JBoss Enterprise Application Platform. **CVE-2026-1002**: A flaw was found in Vert.x. The Web static handler component cache can be manipulated to deny the access to static files served by the handler using specifically crafted request URIs, preventing legitimate users from accessing static files with an HTTP 404 response. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:4761

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-23554)
Description	Citrix has released a security update addressing a vulnerability that exists in XenServer products. **CVE-2026-23554**: An issue has been identified in XenServer 8.4 that may allow privileged code in a guest VM to compromise the host. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	XenServer version 8.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696350&articleURL=XenServer_Security_Update_for_CVE_2026_23554

Affected Product	**MongoDB**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4148, CVE-2026-4147)
Description	MongoDB has released security updates addressing multiple vulnerabilities that exist in MongoDB Server. **CVE-2026-4148**: A use-after-free vulnerability can be triggered in sharded clusters by an authenticated user with the read role who issues a specially crafted $lookup or $graphLookup aggregation pipeline. **CVE-2026-4147**: An authenticated user with the read role may read limited amounts of uninitialized stack memory via specially-crafted issuances of the filemd5 command. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB Server Versions: • 7.0 affects versions prior to 7.0.31 • 8.0 affects versions prior to 8.0.20 • 8.2 affects versions prior to 8.2.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://jira.mongodb.org/browse/SERVER-119319 • https://jira.mongodb.org/browse/SERVER-119317

Affected Product	**IBM**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-24515, CVE-2026-25210)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-24515**: In libexpat before 2.7.4, XML_ExternalEntityParserCreate does not copy unknown encoding handler user data. **CVE-2026-25210**: In libexpat before 2.7.4, the doContent function does not properly determine the buffer size bufSize because there is no integer overflow check for tag buffer reallocation. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AIX versions 7.3 VIOS versions 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7266568 • https://www.ibm.com/support/pages/node/7266572

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12680, CVE-2025-12679, CVE-2025-12772, CVE-2025-12773)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE SANnav Management Software. 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 SANnav Management Software - Prior to v2.4.0b
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst05000en_us&docLocale=en_US

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.