Advisory Alert

Alert Number: AAA20260429 **Date:** April 29, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	HTTP Request/Response Smuggling Vulnerability
Citrix	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	HTTP Request/Response Smuggling Vulnerability (CVE-2026-1525)
Description	IBM has released a security update addressing a vulnerability that exists in their Cloud Pak products. **CVE-2026-1525**: Undici allows duplicate HTTP Content-Length headers when they are provided in an array with case-variant names (e.g., Content-Length and content-length). This produces malformed HTTP/1.1 requests with multiple conflicting Content-Length values on the wire. Denial of Service: Strict HTTP parsers (proxies, servers) will reject requests with duplicate Content-Length headers (400 Bad Request) * HTTP Request Smuggling: In deployments where an intermediary and backend interpret duplicate headers inconsistently (e.g., one uses the first value, the other uses the last), this can enable request smuggling attacks leading to ACL bypass, cache poisoning, or credential hijacking. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Decision Optimization for Cloud Pak for Data versions 5.0 through 5.3.1 releases
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7271000

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23558, CVE-2026-23556, CVE-2026-23559, CVE-2026-23560, CVE-2026-23561, CVE-2025-54505)
Description	Citrix 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. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	XenServer 8.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696527&articleURL=XenServer_Security_Update_for_Multiple_Issues

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796, CVE-2026-35155)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their iDRAC 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	iDRAC9 Versions : • prior to 7.30.10.50 • prior to 7.00.00.184 iDRAC10 Versions : • prior to 1.30.10.50 • 1.20.70.50 and 1.30.05.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000452302/dsa-2026-154-security-update-for-dell-idrac9-and-idrac10-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000452298/dsa-2026-187-security-update-for-dell-idrac10-vulnerability

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-27601, CVE-2025-69873, CVE-2026-1526, CVE-2026-1527, CVE-2026-1528, CVE-2026-2229, CVE-2026-2581, CVE-2026-24842, CVE-2026-26996, CVE-2026-0540, CVE-2025-68157, CVE-2025-68458, CVE-2026-25128, CVE-2026-2391, CVE-2026-3449, CVE-2026-25639, CVE-2026-2327)
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	Decision Optimization for Cloud Pak for Data versions 5.0 through 5.3.1 releases Platform Navigator in IBM Cloud Pak for Integration (CP4I) versions : • 16.1.0 to 16.1.0.21 • 16.1.1 • 16.1.2 • 16.1.3 to 16.1.3.3 Automation Assets in IBM Cloud Pak for Integration (CP4I) : • 4.0.0-sc2 to 4.0.17-sc2 • 4.1.0 • 4.2.0 • 4.3.0 • 4.3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7270996 • https://www.ibm.com/support/pages/node/7271000

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.