Advisory Alert

Alert Number: AAA20260324 **Date:** March 24, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	HTTP Request Smuggling Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing vulnerabilities that exist in third-party components utilized by their products. These vulnerabilities could be exploited by malicious users to conduct Path Traversal, Cross Site Scripting and Remote Code Execution attacks. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Secure Connect Gateway-Application versions 5.28.00.00 through 5.32.00.00 Secure Connect Gateway –Appliance • Versions between v5.28.00.00 and v5.32.00.004 • Versions prior to 5.34.00.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000438589/dsa-2026-020-security-update-for-dell-secure-connect-gateway-application-and-appliance-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000443243/dsa-2026-152-dell-secure-connect-gateway-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-3055, CVE-2026-4368)
Description	Citrix has released a security update addressing multiple vulnerabilities that exists in their products. **CVE-2026-3055**: Insufficient input validation leading to memory overread. Citrix ADC or Citrix Gateway must be configured as a SAML IDP. **CVE-2026-4368**: Race Condition leading to User Session Mixup. Citrix ADC or Citrix Gateway must be configured as a Gateway or AAA virtual server. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-66.59 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-62.23 NetScaler ADC FIPS and NDcPP BEFORE 13.1-37.262
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696300

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing 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 Real Time Module 15-SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise High Performance Computing 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260970-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260967-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260964-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260962-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260961-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260958-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260954-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-53066, CVE-2025-53057, CVE-2026-22029, CVE-2025-46394, CVE-2024-58251, CVE-2025-5987, CVE-2026-25639, CVE-2025-68470, CVE-2025-9230, CVE-2025-13473, CVE-2025-14550, CVE-2026-1207, CVE-2026-1285, CVE-2026-1287, CVE-2026-1312)
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 Storage Insights - Data Collector version 20240303-0731 IBM Storage Defender - Resiliency Service versions 2.0.0 to 2.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7267131 • https://www.ibm.com/support/pages/node/7266676

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	HTTP Request Smuggling Vulnerability (CVE-2026-1002)
Description	Red Hat has released a security update addressing a vulnerability that exists in JBoss Enterprise Application products. **CVE-2026-1002**: The Vert.x Web static handler component cache can be manipulated to deny the access to static files served by the handler using specifically crafted request URI. The issue comes from an improper implementation of the C. rule of section 5.2.4 of RFC3986 and is fixed in Vert.x Core component. 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-2026:5482

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.