Advisory Alert

Alert Number: AAA20260129 **Date:** January 29, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	**Multiple Vulnerabilities**
Dell	**Critical**	**Multiple Vulnerabilities**
Solar Winds	**Critical**	**Multiple Vulnerabilities**
Solar Winds	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Check Point	**Medium**	Information Disclosure Vulnerabilities
Citrix	**Medium**	Multiple Vulnerabilities
Drupal	**Low**	XML Element Injection Vulnerability

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released a security update addressing multiple vulnerabilities that exist in Session Smart Routers. These vulnerabilities could be exploited by malicious users to compromise the affected system. Juniper advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Session Smart Router versions prior to 6.2.10-lts and 6.3.7-sts
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://supportportal.juniper.net/s/article/On-Demand-Security-Bulletin-Multiple-vulnerabilities-resolved-in-Session-Smart-Router-6-2-10-lts-6-3-7-sts

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that are present in third-party products used in Dell OpenManage Network Integration. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell OpenManage Network Integration versions prior to 3.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000420893/dsa-2026-045-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities

Affected Product	**Solar Winds**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40552, CVE-2025-40551, CVE-2025-40554, CVE-2025-40553)
Description	Solar Winds has released a security update addressing multiple vulnerabilities that exist in the SolarWinds Web Help Desk product. These vulnerabilities could be exploited by malicious users to conduct authentication bypass and remote code execution. Solar Winds advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SolarWinds Web Help Desk versions prior and including 12.8.8 HF1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40552 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40551 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40554 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40553

Affected Product	**Solar Winds**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40537, CVE-2025-40536)
Description	Solar Winds has released a security update addressing multiple vulnerabilities that exist in the SolarWinds Web Help Desk product. **CVE-2025-40537:** SolarWinds Web Help Desk was found to be susceptible to a hardcoded credentials vulnerability that, under certain situations, could allow access to administrative functions. **CVE-2025-40536**: SolarWinds Web Help Desk was found to be susceptible to a security control bypass vulnerability that if exploited, could allow an unauthenticated attacker to gain access to certain restricted functionality. Solar Winds advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SolarWinds Web Help Desk versions prior and including 12.8.8 HF1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40537 • https://www.solarwinds.com/trust-center/security-advisories/cve-2025-40536

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39898, CVE-2025-39993, CVE-2023-53705, CVE-2025-40248, CVE-2023-53751, CVE-2025-40277)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in Red Hat Enterprise Linux Server. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:1512

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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 system. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Basesystem Module 15-SP7 Development Tools Module 15-SP7 Legacy Module 15-SP7 openSUSE Leap 15.5 SUSE Linux Enterprise Desktop 15 SP7 SUSE Linux Enterprise High Availability Extension 15 SP7 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP5 LTSS SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP7 SUSE Linux Enterprise Workstation Extension 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20260317-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260316-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20260315-1/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-12758, CVE-2025-56200, CVE-2024-13009, CVE-2024-6763, CVE-2021-23413, CVE-2025-24970, CVE-2024-47535, CVE-2025-25193, CVE-2025-58457, CVE-2025-66221, CVE-2025-66418, CVE-2025-66471, CVE-2026-21441, CVE-2024-10976, CVE-2024-10979, CVE-2024-10977, CVE-2024-7348, CVE-2024-10978, CVE-2025-11083, CVE-2025-9086, CVE-2025-64720, CVE-2025-65018, CVE-2025-66293, CVE-2025-39697, CVE-2025-39971, CVE-2025-14914)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service, Privilege Escalation, Cross-site Scripting, Buffer Overflow, and Path Traversal. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar User Behavior Analytics versions 1.0.0 to 5.0.3 QRadar versions 7.5.0 to 7.5.0 UP14 IF03 IBM WebSphere Application Server Liberty versions 17.0.0.3 to 26.0.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7258232 • https://www.ibm.com/support/pages/node/7258234 • https://www.ibm.com/support/pages/node/7258224

Affected Product	**Check Point**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerabilities (CVE-2025-8304, CVE-2025-8305)
Description	Check Point has released a security update addressing multiple information disclosure vulnerabilities that exist in Identity Agent for a Terminal Server. **CVE-2025-8304**: An authenticated local user can obtain information that allows claiming security policy rules of another user due to sensitive information being accessible in the Windows Registry keys for Check Point Identity Agent running on a Terminal Server. **CVE-2025-8305**: An authenticated local user can obtain information that allows claiming security policy rules of another user due to sensitive information being printed in plaintext in Identity Agent for Terminal Services debug files. Check Point advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Identity Agent for a Terminal Server versions prior to 81.084.0000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.checkpoint.com/results/sk/sk184263 • https://support.checkpoint.com/results/sk/sk184264

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-58151, CVE-2026-23553)
Description	Citrix has released a security update addressing multiple vulnerabilities that exist in XenServer **CVE-2025-58151**: This vulnerability may allow privileged code in a guest VM to cause the host to become slow or unresponsive to management operations. **CVE-2026-23553**: This vulnerability may allow code in a guest VM process to infer in-memory data of a different process running within that same VM. 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=CTX695997&articleURL=XenServer_Security_Update_for_CVE_2025_58151_and_CVE_2026_23553

Affected Product	**Drupal**
Severity	**Low**
Affected Vulnerability	XML Injection Vulnerability (CVE-2026-1554)
Description	Drupal has released a security update addressing an xml injection vulnerability that exists in the Central Authentication System (CAS) module. **CVE-2026-1554**: The module doesn't sufficiently sanitize user-supplied field values configured to be included as attributes in a CAS server response. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	CAS Server versions below 2.0.3 and 2.1.1 and 2.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-007

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.