Advisory Alert

Alert Number: AAA20250807 **Date:** August 7, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary File Write In Archive Extraction Vulnerability
Dell	**High**	Multiple Vulnerabilities
NetApp	**High**	Privilege Escalation Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary File Write In Archive Extraction Vulnerability (CVE-2025-4517)
Description	IBM has released security updates addressing an Arbitrary File Write In Archive Extraction Vulnerability that exists in IBM QRadar SIEM. **CVE-2025-4517** - Allows arbitrary filesystem writes outside the extraction directory during extraction with filter="data". You are affected by this vulnerability if using the tarfile module to extract untrusted tar archives using TarFile.extractall() or TarFile.extract() using the filter= parameter with a value of "data" or "tar". IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP12 IF03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7241589

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38747, CVE-2025-38746)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell SupportAssist OS Recovery. **CVE-2025-38747** - Dell SupportAssist OS Recovery, versions prior to 5.5.14.0, contain a Creation of Temporary File With Insecure Permissions vulnerability. A local authenticated attacker could potentially exploit this vulnerability, leading to Elevation of Privileges. **CVE-2025-38746** - Dell SupportAssist OS Recovery, versions prior to 5.5.14.0, contains an Exposure of Sensitive Information to an Unauthorized Actor vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Information Disclosure. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell SupportAssist OS Recovery versions prior to 5.5.14.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000353093/dsa-2025-315

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-26513)
Description	NetApp has released security updates addressing a Privilege Escalation Vulnerability that exists in SAN Host Utilities for Windows. **CVE-2025-26513** - The installer for SAN Host Utilities for Windows versions prior to 8.0 is susceptible to a vulnerability which when successfully exploited could allow a local user to escalate their privileges which causes disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAN Host Utilities for Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250806-0001

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47527, CVE-2022-48669, CVE-2022-49395, CVE-2022-49788, CVE-2023-52451, CVE-2023-52764, CVE-2023-52877, CVE-2024-26659, CVE-2024-26934, CVE-2024-26964, CVE-2024-27059, CVE-2024-36945, CVE-2024-43888, CVE-2024-57980, CVE-2024-58002, CVE-2025-21727, CVE-2025-21928, CVE-2025-21991, CVE-2025-37890, CVE-2025-37958, CVE-2025-38052)
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 system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64, AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:13135 • https://access.redhat.com/errata/RHSA-2025:13120

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-40403, CVE-2024-12243, CVE-2025-3576, CVE-2024-47554, CVE-2024-31141, CVE-2022-48919, CVE-2024-50301, CVE-2024-53064, CVE-2025-21764, CVE-2025-27817, CVE-2025-27818, CVE-2025-32462, CVE-2024-12718, CVE-2025-4138, CVE-2025-4330, CVE-2025-4435, CVE-2023-2976, CVE-2020-8908, CVE-2024-12133, CVE-2025-6020, CVE-2025-4802, CVE-2024-52894)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM and Db2 server. These vulnerabilities could be exploited by malicious users to cause Denial of Service, data modification, Information Disclosure, Arbitrary Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP12 IF03 IBM Db2 server versions 10.5.0.0 - 10.5.0.11, 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7241589 • https://www.ibm.com/support/pages/node/7240953

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20331, CVE-2025-20332)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco Identity Services Engine. **CVE-2025-20331** - This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE-2025-20332** - This vulnerability is due to the lack of server-side validation of Administrator permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to an affected system. A successful exploit could allow the attacker to modify descriptions of files on a specific page. To exploit this vulnerability, an attacker would need valid read-only Administrator credentials. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE Releases 3.4, 3.3, 3.2, 3.1, 3.0 and earlier Cisco ISE-PIC Release 3.3, 3.1, 3.0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise_xss_acc_cont-YsR4uT4U

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.