Advisory Alert

Alert Number: AAA20251208 **Date:** December 8, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Deserialization of Untrusted Data Vulnerability
NetApp	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Synology	**Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Apache HTTP Server	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-9681, CVE-2025-0725, CVE-2025-4748, CVE-2023-4807, CVE-2023-0464, CVE-2023-2650, CVE-2024-0727, CVE-2023-3817, CVE-2023-5678, CVE-2023-0465, CVE-2023-0466, CVE-2025-30219, CVE-2025-29087, CVE-2025-6965)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party components present in Dell Networker 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	Networker Server, NetWorker Client, NetWorker Storage Node versions: • prior to 19.12.0.4 • 19.13 through 19.13.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000400319/dsa-2025-335-security-update-for-dell-networker-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Deserialization of Untrusted Data Vulnerability (CVE-2025-30065)
Description	IBM has released a security update addressing a deserialization of untrusted data vulnerability that exists within IBM Storage Protect Server. **CVE-2025-30065:** Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code IBM advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	IBM Storage Protect Server versions 8.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7249983

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-8714, CVE-2025-8715, CVE-2025-32415, CVE-2025-24855, CVE-2023-39615, CVE-2025-6021, CVE-2024-55549)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS), Information Disclosure and Data Modification. NetApp advises to apply this security fixes at your earliest to protect your systems from potential threats.
Affected Products	Brocade SAN Navigator (SANnav) NetApp Manageability SDK ONTAP 9 ONTAP tools for VMware vSphere 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20251205-0005 • https://security.netapp.com/advisory/ntap-20251205-0004 • https://security.netapp.com/advisory/ntap-20250605-0003 • https://security.netapp.com/advisory/ntap-20250613-0006 • https://security.netapp.com/advisory/ntap-20250801-0009 • https://security.netapp.com/advisory/ntap-20250711-0009 • https://security.netapp.com/advisory/ntap-20250613-0007

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Denial of Service (DoS), Arbitrary Code Execution, Information Disclosure, Authentication Bypass, and Code Injection. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• IBM Storage Protect Server versions 8.1 • IBM QRadar SIEM versions 7.5 - 7.5.0 UP14 IF01 • IBM Storage Protect Operations Center versions 8.1 • IBM Storage Protect for Space Management versions 8.1.0.0 - 8.1.27.1 • IBM Storage Protect for Virtual Environments: Data Protection for Hyper-V versions 8.1.0.0 - 8.1.27.1 • IBM Storage Protect for Virtual Environments: Data Protection for VMware versions 8.1.0.0 - 8.1.27.1 • IBM Storage Protect Client versions 8.1.0.0 - 8.1.27.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7249982 • https://www.ibm.com/support/pages/node/7249983 • https://www.ibm.com/support/pages/node/7253912 • https://www.ibm.com/support/pages/node/7249990 • https://www.ibm.com/support/pages/node/7249995 • https://www.ibm.com/support/pages/node/7253904 • https://www.ibm.com/support/pages/node/7253908 • https://www.ibm.com/support/pages/node/7253907

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-66592, CVE-2025-66593)
Description	Synology has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-66592, CVE-2025-66593:** allows local users to write arbitrary files with restricted content. Synology advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Synology Active Backup for Business Agent versions prior to 3.1.0-4967 Synology Assistant versions prior to 7.0.6-50085
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.synology.com/en-global/security/advisory/Synology_SA_25_16 • https://www.synology.com/en-global/security/advisory/Synology_SA_25_17

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53401, CVE-2023-53539, CVE-2022-50543, CVE-2025-39966)
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 systems. Red Hat advises to apply this security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:22801 • https://access.redhat.com/errata/RHSA-2025:22802

Affected Product	**Apache HTTP Server**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-55753, CVE-2025-58098, CVE-2025-59775, CVE-2025-65082, CVE-2025-66200)
Description	ASF has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to conduct Information Disclosure, Buffer Overflow and Server-Side Request Forgery. ASF advises to apply this security fixes at your earliest to protect your systems from potential threats.
Affected Products	Apache HTTP Server versions prior to 2.4.66
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

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.