Advisory Alert

Alert Number: AAA20251117 **Date:** November 17, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Security Update
Fortinet	**Critical**	Relative Path Traversal Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**Medium**	Improper Allocation Of Resources Vulnerability

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2025-23048)
Description	NetApp has released security update addressing a vulnerability that exist in apache HTTP server which intern-effect netapp products. These vulnerabilities could be exploited by malicious users to cause 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	ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250718-0013

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Relative Path Traversal Vulnerability (CVE-2025-64446)
Description	FortiGuard has released security update addressing a relative path traversal vulnerability that exists their products. **CVE-2025-64446 -** A relative path traversal vulnerability in FortiWeb may allow an unauthenticated attacker to execute administrative commands on the system via crafted HTTP or HTTPS requests FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiWeb 8.0 Versions - 8.0.0 through 8.0.1 FortiWeb 7.6 Versions - 7.6.0 through 7.6.4 FortiWeb 7.4 Versions - 7.4.0 through 7.4.9 FortiWeb 7.2 Versions - 7.2.0 through 7.2.11 FortiWeb 7.0 Versions - 7.0.0 through 7.0.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-25-910

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell VxRail Appliance Versions - 7.0.000 through 7.0.541 and 8.0.000 through 8.0.330
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000325586/dsa-2025-215-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000335212/dsa-2025-244-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-42516, CVE-2024-43204, CVE-2024-43394, CVE-2024-47252, CVE-2025-49630, CVE-2025-49812, CVE-2025-53020, CVE-2022-2625, CVE-2025-1053, CVE-2025-27152)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, disclosure of sensitive information and addition or modification of data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP 9 NetApp Shift Toolkit Brocade SAN Navigator (SANnav) Prior to 2.2.2a and 2.3.0. Brocade SAN Navigator (SANnav) Prior to SANnav 2.4.0 and 2.3.1b.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250718-0013 • https://security.netapp.com/advisory/ntap-20251114-0014 • https://security.netapp.com/advisory/ntap-20251114-0005 • https://security.netapp.com/advisory/ntap-20251114-0004

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38796, CVE-2024-21859, CVE-2024-31155, CVE-2024-37020, CVE-2024-25571, CVE-2024-39279, CVE-2024-28047, CVE-2024-31068, CVE-2025-22397, CVE-2025-3360, CVE-2025-31115, CVE-2024-56171, CVE-2025-24928, CVE-2025-27113, CVE-2024-35195, CVE-2022-40899, CVE-2024-6345, CVE-2023-7104, CVE-2024-7592, CVE-2024-6232, CVE-2024-3219, CVE-2024-6923, CVE-2024-2511, CVE-2024-37891, CVE-2023-32681, CVE-2024-47611, CVE-2020-22916)
Description	Dell has released security updates addressing multiple vulnerabilities that exist their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell APEX Cloud Platform for Red Hat OpenShift Versions - prior to 03.04.01.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000321006/dsa-2025-196-security-update-for-dell-apex-cloud-platform-for-red-hat-openshift-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Improper Allocation Of Resources Vulnerability (CVE-2025-36008)
Description	IBM has released security updates addressing an improper allocation of resources vulnerability that exists in their products. **CVE-2025-36008 -** IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) could allow an authenticated user to cause a denial of service due to improper allocation of resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Versions - 11.5.0 - 11.5.9, 12.1.0 - 12.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7250482

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.