Advisory Alert

Alert Number: AAA20250704 **Date:** July 4, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Linux Kernel Vulnerability
NetApp	**High**	Denial of Service Vulnerability
IBM	**High**, Medium	Multiple Vulnerabilities
PHP	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Data Protection Advisor. 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 Protection Advisor Versions 19.12 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000340538/dsa-2025-276-security-update-for-data-protection-advisor-for-multiple-vulnerabilities

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Linux Kernel Vulnerability (CVE-2024-47685)
Description	NetApp has released security updates addressing a Linux Kernel Vulnerability that exists in their products. **CVE-2024-47685** - Multiple NetApp products incorporate Linux kernel. Certain versions of Linux kernels are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere ONTAP tools for VMware vSphere 10 E-Series SANtricity OS Controller Software 11.x StorageGRID (formerly StorageGRID Webscale) NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S NetApp HCI Baseboard Management Controller (BMC) - H410C StorageGRID Baseboard Management Controller (BMC) - SG6060/SGF6024/SG100/SG1000 NetApp HCI Compute Node (Bootstrap OS)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250613-0011

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-53580)
Description	NetApp has released security updates addressing a Denial of Service Vulnerability that exists in a third party product which affects ONTAP 9. **CVE-2024-53580** - Multiple NetApp products incorporate iperf3. iperf3 version 3.17.1 is susceptible to a vulnerability which when successfully exploited could lead to 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-20250404-0009

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27664, CVE-2022-41721, CVE-2022-32149, CVE-2022-23648, CVE-2021-43816, CVE-2023-39325, CVE-2022-21698, CVE-2025-4447, CVE-2024-27289)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM DB2 modules. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure, SQL Injection, data modification. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Client and Server versions 10.5.0.0 - 10.5.0.11, 11.1.0 - 11.1.4.7 and 11.5.0 - 11.5.9 IBM DB2 Data Management Console versions 3.1.11.x - 3.1.13 IBM DB2 Data Management Console on CPD versions 4.7.x to 4.8.8 and 5.0.x to 5.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7238830 • https://www.ibm.com/support/pages/node/7238831 • https://www.ibm.com/support/pages/node/7238833 • https://www.ibm.com/support/pages/node/7238146

Affected Product	**PHP**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6491, CVE-2025-1220, CVE-2025-1735)
Description	PHP Group has released security updates addressing multiple vulnerabilities that exist in some php modules and functions. **CVE-2025-6491** - Libxml versions prior to 2.13 cannot correctly handle a call to xmlNodeSetName() with a name longer than 2G. It will leave the node object in an invalid state with a NULL name. This later causes a NULL pointer dereference when using the name during message serialization. **CVE-2025-1220** - fsockopen() doesn't regard hostname as well, hostname is terminated at the null byte. This can cause Server Side Request Forgery in general case. During fsockopen is being called hostname is passed directly to the low-level C function calls. **CVE-2025-1735** - Missing error checking could result in SQL injection and missing error handling could lead to crashes due to null pointer dereferences. PHP Group advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	php 8.1 versions prior to 8.1.33 php 8.2 versions prior to 8.2.29 php 8.3 versions prior to 8.3.23 php 8.4 versions prior to 8.4.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.php.net/ChangeLog-8.php#8.3.23 • https://www.php.net/ChangeLog-8.php#8.1.33 • https://www.php.net/ChangeLog-8.php#8.2.29 • https://www.php.net/ChangeLog-8.php#8.4.10

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.