Advisory Alert

Alert Number: AAA20250623 **Date:** June 23, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
NetApp	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
F5	**High**	HTTP Request Smuggling Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**NetApp**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-24531, CVE-2025-24813, CVE-2024-47685)
Description	NetApp has released security updates addressing multiple vulnerabilities that exists in their products. **CVE-2023-24531**- A command injection vulnerability in Go's go env command—it outputs environment values as a shell script without sanitizing them, allowing crafted variables to execute arbitrary commands or inject unauthorized environment variables. **CVE-2025-24813** - A path equivalence vulnerability in Apache Tomcat's default servlet (with write-enabled and partial PUT support) could allow unauthenticated attackers to upload or modify files, leading to remote code execution or unauthorized information disclosure. **CVE-2024-47685** - A vulnerability in the Linux kernel's IPv6 Netfilter component—specifically in the nf_reject_ip6_tcphdr_put() function—causes uninitialized TCP header bits (the four reserved "res1" bits) to be sent during IPv6 TCP resets. This can lead to data leakage or instability under IPv6 networking conditions. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere E-Series SANtricity OS Controller Software 11.x NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S/H410C NetApp HCI Compute Node (Bootstrap OS) StorageGRID Baseboard Management Controller (BMC) - SG6060/SGF6024/SG100/SG1000 Trident Trident Autosupport
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250328-0005 • https://security.netapp.com/advisory/ntap-20250321-0001 • https://security.netapp.com/advisory/ntap-20250613-0011

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20599, CVE-2023-6780, CVE-2024-28047, CVE-2024-2961, CVE-2024-31068, CVE-2024-36293, CVE-2024-36347, CVE-2024-38796, CVE-2024-39279, CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-50602, CVE-2024-52533, CVE-2024-56161, CVE-2025-22396, CVE-2025-22397, CVE-2025-26466)
Description	Dell 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. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerEdge BIOS –16G AMD R6625 and R7625- Versions prior to 1.11.2 Dell PowerEdge BIOS –15G AMD R6525- Versions prior to 2.18.1 Dell PowerEdge BIOS –15G R650 and R750- Versions prior to 1.16.2 Dell PowerEdge BIOS –16G R660 and R760- Versions prior to 2.5.4 Dell PowerEdge BIOS –14G R640, R740, R840- Versions prior to 2.23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000334768/dsa-2025-251-security-update-for-dell-vxflex-ready-node-and-powerflex-custom-node-multiple-third-party-component-vulnerabilities

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	HTTP Request Smuggling Vulnerability (CVE-2024-47220)
Description	F5 has released security update addressing a vulnerability that exists in their product. **CVE-2024-47220** - A flaw in WEBrick (versions up to 1.8.1) allows an attacker to include both Content-Length and Transfer-Encoding headers in a single HTTP request. This mismatch enables HTTP request smuggling, where hidden requests (e.g., GET /admin) can be smuggled inside other ones. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next CNF - 1.1.0 - 1.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000151740

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3807, CVE-2021-44906, CVE-2022-3517, CVE-2024-10917, CVE-2024-12797, CVE-2024-21208, CVE-2024-21210, CVE-2024-21217, CVE-2024-21235, CVE-2024-40094, CVE-2024-47535, CVE-2024-56201, CVE-2024-56326, CVE-2024-6119, CVE-2025-1470, CVE-2025-1471, CVE-2025-23184, CVE-2025-25193, CVE-2025-27144, CVE-2025-27516, CVE-2025-3319)
Description	IBM has released a security update addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to man-in-the-middle attacks, denial of service, or unauthorized access. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect for Virtual Environments: Data Protection for Hyper-V - 8.1.0.0 - 8.1.26.0 IBM Storage Protect for Space Management - 8.1.0.0 - 8.1.26.0 IBM Storage Fusion Data Foundation - 4.18.4, 4.19 IBM Storage Protect Plus File Systems Agent - 10.1.6 - 10.1.17 IBM Storage Protect Backup-Archive Client - 8.1.0.000 - 8.1.26.xxx IBM Storage Protect Server - 8.1.0.000 - 8.1.26.000 IBM Storage Protect Operations Center - 8.1.0.000 - 8.1.26.xxx
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7237492 • https://www.ibm.com/support/pages/node/7236997 • https://www.ibm.com/support/pages/node/7236998 • https://www.ibm.com/support/pages/node/7236993 • https://www.ibm.com/support/pages/node/7237493 • https://www.ibm.com/support/pages/node/7237491 • https://www.ibm.com/support/pages/node/7237440 • https://www.ibm.com/support/pages/node/7237323 • https://www.ibm.com/support/pages/node/7237331 • https://www.ibm.com/support/pages/node/7237325 • https://www.ibm.com/support/pages/node/7237492 • https://www.ibm.com/support/pages/node/7236999 • https://www.ibm.com/support/pages/node/7237002 • https://www.ibm.com/support/pages/node/7237001 • https://www.ibm.com/support/pages/node/7236993 • https://www.ibm.com/support/pages/node/7237329

Affected Product	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1147, CVE-2023-39975, CVE-2024-20968, CVE-2024-11187, CVE-2024-0450, CVE-2024-11168, CVE-2025-0395, CVE-2024-7409, CVE-2024-38820, CVE-2024-3447, CVE-2025-1178, CVE-2025-4947, CVE-2024-47814, CVE-2025-5025, CVE-2025-22871)
Description	NetApp has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for Microsoft Windows Active IQ Unified Manager for VMware vSphere NetApp HCI Baseboard Management Controller (BMC) - H300S/H500S/H700S/H410S/ H410C/ H610S/ H615C NetApp HCI Compute Node (Bootstrap OS) OnCommand Insight OnCommand Workflow Automation ONTAP tools for VMware vSphere 10 SnapCenter
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20250404-0003 • https://security.netapp.com/advisory/ntap-20240201-0008 • https://security.netapp.com/advisory/ntap-20250207-0002 • https://security.netapp.com/advisory/ntap-20250328-0005 • https://security.netapp.com/advisory/ntap-20250411-0005 • https://security.netapp.com/advisory/ntap-20250411-0004 • https://security.netapp.com/advisory/ntap-20250321-0001 • https://security.netapp.com/advisory/ntap-20250228-0006 • https://security.netapp.com/advisory/ntap-20250502-0008 • https://security.netapp.com/advisory/ntap-20241129-0003 • https://security.netapp.com/advisory/ntap-20250425-0005 • https://security.netapp.com/advisory/ntap-20250411-0008 • https://security.netapp.com/advisory/ntap-20250620-0009 • https://security.netapp.com/advisory/ntap-20250411-0009 • https://security.netapp.com/advisory/ntap-20250613-0011 • https://security.netapp.com/advisory/ntap-20250620-0008 • https://security.netapp.com/advisory/ntap-20250530-0004

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.