Advisory Alert

Alert Number: AAA20241014 **Date:** October 14, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NETGEAR	**High**, **Medium**	Multiple Vulnerabilities
Dell	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40898, CVE-2024-36387, CVE-2024-39884, CVE-2024-40725, CVE-2024-38472, CVE-2024-38473, CVE-2024-38474, CVE-2024-38475, CVE-2024-38476, CVE-2024-38477, CVE-2024-39573, CVE-2023-38709, CVE-2024-24795, CVE-2024-27316, CVE-2024-24549, CVE-2024-23672, CVE-2024-34750, CVE-2023-46218, CVE-2023-46219, CVE-2024-29736, CVE-2024-32007)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products which in turn affect Dell 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 NetWorker Management Console (NMC) Version 19.10.0.4 and prior Dell NetWorker Authentication Service Version 19.10.0.4 and prior Dell NetWorker Server Version 19.10.0.4 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000235068/dsa-2024-423-security-update-for-dell-networker-and-networker-management-console-nmc-multiple-component-vulnerabilities

Affected Product	**NETGEAR**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	NETGEAR has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause post-authentication buffer overflow, authentication bypass, security misconfiguration, post-authentication command injection. NETGEAR advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	CAX30 fixed in firmware version 2.2.2.2 MK62 fixed in firmware version 1.7.134 MK72 fixed in firmware version 1.0.3.32 MK82 fixed in firmware version 1.1.7.14 MR60 fixed in firmware version 1.7.134 MR70 fixed in firmware version 1.0.3.32 MR80 fixed in firmware version 1.1.7.14 MS60 fixed in firmware version 1.7.134 MS70 fixed in firmware version 1.0.3.32 MS80 fixed in firmware version 1.1.7.14 R6700v3 fixed in firmware version 1.0.4.128 R7000 fixed in firmware version 1.0.11.216 R8000 fixed in firmware version 1.0.4.84 RAX41 fixed in firmware version 1.0.16.132 RAX42 fixed in firmware version 1.0.16.132 RAX43 fixed in firmware version 1.0.16.132 RAX50 fixed in firmware version 1.0.16.132 RAX50S fixed in firmware version 1.0.16.132 RAXE450 fixed in firmware version 1.0.12.96 RAXE500 fixed in firmware version 1.0.12.96 XR1000 fixed in firmware version 1.0.0.72
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://kb.netgear.com/000066257/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2022-0171 • https://kb.netgear.com/000066258/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2022-0201 • https://kb.netgear.com/000066259/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-and-WiFi-Systems-PSV-2022-0202 • https://kb.netgear.com/000066260/Security-Advisory-for-Post-Authentication-Buffer-Overflow-on-Some-Routers-PSV-2023-0079 • https://kb.netgear.com/000066261/Security-Advisory-for-Authentication-Bypass-on-Some-Routers-PSV-2023-0113 • https://kb.netgear.com/000066262/Security-Advisory-for-Security-Misconfiguration-on-Some-Routers-PSV-2023-0116 • https://kb.netgear.com/000066263/Security-Advisory-for-Post-Authentication-Command-Injection-on-Some-Routers-PSV-2023-0119 • https://kb.netgear.com/000066265/Security-Advisory-for-Authentication-Bypass-on-Some-Cable-Modem-Routers-PSV-2023-0138 • https://kb.netgear.com/000066264/Security-Advisory-for-Stored-Cross-Site-Scripting-on-Some-Routers-PSV-2023-0122

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29469, CVE-2023-28484, CVE-2022-40304, CVE-2022-40303, CVE-2022-40898, CVE-2023-1786, CVE-2022-23491, CVE-2022-4304, CVE-2022-44793, CVE-2020-15862, CVE-2020-15861, CVE-2019-20892, CVE-2015-8100, CVE-2024-6387, CVE-2023-48795, CVE-2024-38433, CVE-2023-29499, CVE-2024-25943, CVE-2024-38303, CVE-2024-38304, CVE-2023-31355, CVE-2024-21978, CVE-2024-21980, CVE-2023-31315, CVE-2024-24853, CVE-2024-24980, CVE-2023-42772, CVE-2023-22351, CVE-2023-25546, CVE-2023-41833, CVE-2023-43753, CVE-2024-21781, CVE-2024-21829, CVE-2024-21871, CVE-2024-24968, CVE-2024-23984, CVE-2024-40898, CVE-2024-36387, CVE-2024-39884, CVE-2024-40725, CVE-2024-38472, CVE-2024-38473, CVE-2024-38474, CVE-2024-38475, CVE-2024-38476, CVE-2024-38477, CVE-2024-39573, CVE-2023-38709, CVE-2024-24795, CVE-2024-27316, CVE-2023-46218, CVE-2023-46219, CVE-2024-29736, CVE-2024-32007, CVE-2024-24549, CVE-2024-23672, CVE-2024-34750)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products which in turn affect Dell 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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000227762/dsa-2024-308-security-update-for-dell-poweredge-server-for-intel-august-2024-security-advisories-2024-3-ipu • https://www.dell.com/support/kbdoc/en-us/000227030/dsa-2024-330-security-update-for-dell-powerprotect-dd-openssh-vulnerability • https://www.dell.com/support/kbdoc/en-us/000228135/dsa-2024-309-security-update-for-dell-poweredge-server-for-improper-input-validation-vulnerability • https://www.dell.com/support/kbdoc/en-us/000228137/dsa-2024-310-security-update-for-dell-poweredge-server-for-access-of-memory-location-after-end-of-buffer-vulnerability • https://www.dell.com/support/kbdoc/en-us/000227518/dsa-2024-306-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000227665/dsa-2024-344-security-update-for-dell-amd-based-poweredge-server-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000223029/dsa-2024-102-security-update-for-dell-technologies-powerprotect-dd-vulnerabilitie

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26614, CVE-2024-36886, CVE-2023-52471)
Description	IBM 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. **CVE-2024-26614** - Linux Kernel is vulnerable to a denial of service, caused by an error related to making sure init the accept_queue's spinlocks once. A local attacker could exploit this vulnerability to cause a denial of service. **CVE-2024-36886** - Linux Kernel could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free when processing fragmented TIPC messages. By sending a specially crafted request, an attacker could exploit this vulnerability to execute code in the context of the kernel. **CVE-2023-52471** - Linux Kernel is vulnerable to a denial of service, caused by a NULL pointer dereference in ice_ptp.c. A local attacker could exploit this vulnerability to cause a denial of service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Copy Data Management 2.2.0.0 - 2.2.24.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7172999

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.