Advisory Alert

Alert Number: **AAA20250131** **Date:** **January 31, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Broadcom VMware	**High**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Kernel Vulnerabilities
SonicWall	**Medium**	Arbitrary System File Read Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3429, CVE-2022-1292, CVE-2022-2068, CVE-2022-4304, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-1786, CVE-2023-31102, CVE-2023-3446, CVE-2023-3817, CVE-2023-40481, CVE-2023-47108, CVE-2023-45142, CVE-2023-52340, CVE-2023-5678, CVE-2024-21853, CVE-2024-21944, CVE-2024-25565, CVE-2024-26782, CVE-2024-37891, CVE-2024-41110, CVE-2024-42154, CVE-2024-44932, CVE-2024-44964, CVE-2024-47757, CVE-2024-50089, CVE-2024-50115, CVE-2024-50125, CVE-2024-50127, CVE-2024-50154, CVE-2024-50205, CVE-2024-50259, CVE-2024-50264, CVE-2024-50267, CVE-2024-50274, CVE-2024-50279, CVE-2024-50290, CVE-2024-50301, CVE-2024-50302, CVE-2024-52530, CVE-2024-52531, CVE-2024-52532, CVE-2024-53061, CVE-2024-53063, CVE-2024-53068, CVE-2024-7348)
Description	Dell has released security updates to address multiple vulnerabilities in their products. If exploited, these vulnerabilities could allow 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 7.0.533 Dell NetWorker Versions - 19.11 through 19.11.0.3 Dell NetWorker Versions - 19.10 through 19.10.0.6 Dell NetWorker Versions - prior to 19.10 Dell NetWorker Virtual Edition NVE-OVA Versions - 19.11 through 19.11.0.2 Dell NetWorker Virtual Edition NVE-OVA Versions - 19.10 through 19.10.0.6 Dell NetWorker Virtual Edition NVE-OVA Versions - prior to 19.10 Dell NetWorker NetWorker Management Console Versions - 19.11 through 19.11.0.2 Dell NetWorker NetWorker Management Console Versions - 19.10 through 19.10.0.6 Dell NetWorker NetWorker Management Console Versions - prior to 19.10 Dell NetWorker NetWorker Management Console Versions - 19.11 through 19.11.0.2 Dell NetWorker NetWorker Management Console Versions - prior to 19.10.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000278811/dsa-2025-064-security-update-for-dell-networker-networker-virtual-edition-and-networker-management-console-multiple-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000278951/dsa-2025-028-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**Broadcom VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22218, CVE-2025-22219, CVE-2025-22220, CVE-2025-22221, CVE-2025-22222)
Description	Broadcom has released security updates addressing multiple vulnerabilities in VMware Aria Operations for logs and VMware Aria Operations. If exploited A malicious actor with View Only Admin permissions may be able to read the credentials of a VMware product integrated with VMware Aria Operations for Logs. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware Aria Operations for logs versions prior to 8.18.3 VMware Aria Operations versions prior to 8.18.3 VMware Cloud Foundation version 5.x, 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/25329

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Kernel Vulnerabilities (CVE-2024-40967, CVE-2024-53164, CVE-2023-21400, CVE-2024-53141, CVE-2024-53103)
Description	Ubuntu has released security updates addressing Kernel Vulnerabilities that exist in their products. If exploited these vulnerabilities could cause denial of service, execute arbitrary code, double-free. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7234-2

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Arbitrary System File Read Vulnerability (CVE-2025-23007)
Description	SonicWall has released security updates addressing an Arbitrary System File Read Vulnerability in their products. **CVE-2025-23007 -** A vulnerability in the NetExtender Windows client log export function allows unauthorized access to sensitive Windows system files, potentially leading to privilege escalation. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetExtender Windows (32 and 64 bit) 10.3.0 and Prior versions.
Officially Acknowledged by the Vendor	Yes
`Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0005

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.