



Advisory Alert

Alert Number: AAA20250801 Date: August 1, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	Critical	Multiple Vulnerabilities
Ubuntu	High, Medium	Multiple Vulnerabilities
Dell	High, Medium	Multiple Vulnerabilities

Description

Affected Product	Dell
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell Avamar, NVE, DPA, Dell NetWorker, PowerProtect Data Domain and DP Series. 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	<ul style="list-style-type: none">https://www.dell.com/support/kbdoc/en-us/000351152/dsa-2025-293-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-multiple-third-party-vulnerabilitieshttps://www.dell.com/support/kbdoc/en-us/000337898/dsa-2025-263-security-update-for-dell-networker-openssl-vulnerabilitieshttps://www.dell.com/support/kbdoc/en-us/000348708/dsa-2025-159-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities

Affected Product	Ubuntu
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53239, CVE-2024-50073, CVE-2024-49950, CVE-2024-49883, CVE-2023-52975, CVE-2025-38083)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux Kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 16.04 Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<ul style="list-style-type: none">https://ubuntu.com/security/notices/USN-7684-1https://ubuntu.com/security/notices/USN-7683-1

Affected Product	Dell						
Severity	High, Medium						
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0395, CVE-2025-0690, CVE-2025-1125, CVE-2025-0689, CVE-2025-0686, CVE-2025-0624, CVE-2025-0622, CVE-2025-0677, CVE-2025-1118, CVE-2025-0725, CVE-2025-0167, CVE-2025-24928, CVE-2025-26465, CVE-2022-24805, CVE-2022-24810, CVE-2020-15861, CVE-2020-15862, CVE-2018-18066, CVE-2019-20892, CVE-2022-24809, CVE-2018-18065, CVE-2022-24808, CVE-2022-24807, CVE-2022-24806, CVE-2008-6123, CVE-2014-3565, CVE-2012-6151, CVE-2014-2285, CVE-2015-8100, CVE-2025-1094, CVE-2017-12172, CVE-2017-15098, CVE-2017-15099, CVE-2025-27113, CVE-2025-41236)						
Description	<p>Dell has released security updates addressing multiple vulnerabilities that exist in NetWorker and PowerStore products. These vulnerabilities could be exploited by malicious users to compromise the affected system.</p> <p>Dell advises to apply security fixes at your earliest to protect systems from potential threats.</p>						
Affected Products	<p>NetWorker vProxy versions 19.12 through 19.12.0.1</p> <p>NetWorker vProxy versions prior to 19.11.0.6</p> <p>NetWorker Management Console versions 19.12 through 19.12.0.1</p> <p>NetWorker Management Console versions prior to 19.11.0.6</p> <p>NetWorker Server, NetWorker Client, NetWorker Storage Node versions 19.12 through 19.12.0.1</p> <p>NetWorker Server, NetWorker Client, NetWorker Storage Node versions prior to 19.11.0.6</p> <p>ESXi versions prior to ESXi70U3w-24784741 running on following products</p> <table><tr><td>PowerStore 1000X</td><td>PowerStore 5000X</td><td>PowerStore 9000X</td></tr><tr><td>PowerStore 3000X</td><td>PowerStore 7000X</td><td></td></tr></table>	PowerStore 1000X	PowerStore 5000X	PowerStore 9000X	PowerStore 3000X	PowerStore 7000X	
PowerStore 1000X	PowerStore 5000X	PowerStore 9000X					
PowerStore 3000X	PowerStore 7000X						
Officially Acknowledged by the Vendor	Yes						
Patch/ Workaround Released	Yes						
Reference	<ul style="list-style-type: none">https://www.dell.com/support/kbdoc/en-us/000337955/dsa-2025-262-security-update-for-dell-networker-vproxy-multiple-third-party-component-vulnerabilitieshttps://www.dell.com/support/kbdoc/en-us/000337925/dsa-2025-221-security-update-for-dell-networker-management-console-multiple-third-party-component-vulnerabilitieshttps://www.dell.com/support/kbdoc/en-us/000338768/dsa-2025-266-security-update-for-dell-networker-libxml2-vulnerabilityhttps://www.dell.com/support/kbdoc/en-us/000351098/dsa-2025-306-dell-powerstore-family-security-update-for-vmware-vulnerabilities						

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.