Advisory Alert

Alert Number: AAA20250410 **Date:** April 10, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
SonicWall	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Drupal	**High**	Multiple Vulnerabilities
Ubuntu	**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 PowerProtect Cyber Recovery. 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 PowerProtect Cyber Recovery prior to 19.18.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000306005/dsa-2025-113-security-update-for-dell-powerprotect-cyber-recovery

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23008, CVE-2025-23009, CVE-2025-23010)
Description	SonicWall has released security updates addressing multiple vulnerabilities that exist in SonicWall NetExtender. These vulnerabilities could be exploited by malicious users to compromise the affected system. **CVE-2025-23008** - SonicWall NetExtender Improper Privilege Management Vulnerability, An improper privilege management vulnerability in the SonicWall NetExtender Windows (32 and 64 bit) client allows a low privileged attacker to modify configurations. **CVE-2025-23009** - SonicWall NetExtender Local Privilege Escalation Vulnerability, A local privilege escalation vulnerability in SonicWall NetExtender Windows (32 and 64 bit) client which allows an attacker to trigger an arbitrary file deletion. **CVE-2025-23010** - SonicWall NetExtender Improper Link Resolution, An Improper Link Resolution Before File Access ('Link Following') vulnerability in SonicWall NetExtender Windows (32 and 64 bit) client which allows an attacker to manipulate file paths. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetExtender Windows (32 and 64 bit) 10.3.1 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0006

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 openSUSE Leap 15.6 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20251180-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20251183-1/

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-3474, CVE-2025-3131)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-3474** - This vulnerability is mitigated by the fact that an attacker must know the machine name of the variant and underlying page, which is not available within the source code of a page. Additionally, only simple blocks can be added or edited, as a more complex block will trigger an error due to missing permissions. **CVE-2025-3131** – The module doesn't sufficiently protect certain routes from CSRF attacks. This vulnerability is mitigated by the fact that an attacker must get a user with the permission "administer eca" to follow to a given site. It can also be mitigated by disabling the "eca_ui" submodule, which leaves ECA functionality intact, but the vulnerable routes will no longer be available. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Panels module version prior to 4.9.0 for Drupal 8.x ECA module version prior 1.1.12 or 2.0.0 later for Drupal 10 or 11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-033 • https://www.drupal.org/sa-contrib-2025-031

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Linux Kernel. These vulnerabilities could be exploited by malicious users to compromise the system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7429-2 • https://ubuntu.com/security/notices/USN-7429-1 • https://ubuntu.com/security/notices/USN-7428-2 • https://ubuntu.com/security/notices/USN-7428-1

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.