Advisory Alert

Alert Number: AAA20250626 **Date:** June 26, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Remote Code Execution Vulnerabilities
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Cisco	Medium	Authorization Bypass Vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerabilities (CVE-2025-20281, CVE-2025-20282)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Their products. **CVE-2025-20281** - This vulnerability affects Cisco ISE and ISE-PIC releases 3.3 and later, regardless of device configuration. This vulnerability does not affect Cisco ISE and ISE-PIC Release 3.2 or earlier. **CVE-2025-20282** - This vulnerability affects only Cisco ISE and ISE-PIC Release 3.4, regardless of device configuration. This vulnerability does not affect Cisco ISE and ISE-PIC Release 3.3 or earlier. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Cisco ISE or ISE-PIC Release Prior to 3.3 Patch 6 ise-apply-CSCwo99449_3.3.0.430_patch4-SPA.tar.gz • Cisco ISE or ISE-PIC Release Prior to 3.4 Patch 2 ise-apply-CSCwo99449_3.4.0.608_patch1-SPA.tar.gz
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities (CVE-2017-5753, CVE-2022-49179, CVE-2022-49545, CVE-2023-2162, CVE-2023-3567, CVE-2023-52973, CVE-2023-52974, CVE-2023-53000, CVE-2024-40937, CVE-2024-50124, CVE-2024-50125, CVE-2024-50127, CVE-2024-50257, CVE-2024-50279, CVE-2024-50301, CVE-2024-53074, CVE-2024-53208, CVE-2024-56582, CVE-2024-56601, CVE-2024-56605, CVE-2025-21700, CVE-2025-21702, CVE-2025-22004)
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in Their products. These vulnerabilities could be exploited by malicious users to cause out-of-bounds access and use-after-free. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.3, 15.4, 15.5, 15.6 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3, 15-SP4, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server 11 SP4, 11 SP4 LTSS EXTREME CORE SUSE Linux Enterprise Server 12 SP5, 15 SP3, 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP4, 15 SP5, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202502098-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502099-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502101-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502107-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502108-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502106-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502110-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502111-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502112-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502113-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502116-1 • https://www.suse.com/support/update/announcement/2025/suse-su-202502117-1

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6675, CVE-2025-6677, CVE-2025-6674, CVE-2025-5682, CVE-2025-48921, CVE-2025-48922, CVE-2025-48923)
Description	Drupal has released security updates addressing Multiple Vulnerabilities that exist in Their products. These vulnerabilities could be exploited by malicious users to cause access bypass, cross site scripting, cross site request forgery. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Enterprise MFA - TFA for Drupal - All versions before 4.8.0, all 5.0.x and 5.1.x versions, and 5.2.0 Klaro Cookie & Consent Management - All versions earlier than 3.0.7 Toc.js - All versions earlier than 3.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-082 • https://www.drupal.org/sa-contrib-2025-080 • https://www.drupal.org/sa-contrib-2025-077

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Their products. These vulnerabilities that 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 Open Manage Network Integration Software - Versions prior to 3.7 iDRAC10 - Versions prior to 1.20.50.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000337238/dsa-2025-257-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000337136/dsa-2025-245-security-update-for-dell-idrac10-vulnerability

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Authorization Bypass Vulnerability (CVE-2025-20264)
Description	Cisco has released security update addressing an authorization bypass vulnerability that exists in Their products. **CVE-2025-20264** - A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to bypass the authorization mechanisms for specific administrative functions. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE - Versions 3.1 and earlier, 3.3, 3.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-auth-bypass-mVfKVQAU

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.