# Advisory Alert

**Alert Number:** AAA20250522 **Date:** May 22, 2025

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Oracle** | **Critical** | Multiple Vulnerabilities |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Cisco** | **High**, Medium | Multiple Vulnerabilities |
| **Oracle** | **High**, Medium, Low | Multiple Vulnerabilities |
| **cPanel** | **High**, Medium, Low | Multiple Vulnerabilities |
| **F5** | Medium | Denial of Service Vulnerability |
| **Drupal** | Medium, Low | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Oracle** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-11053, CVE-2024-40896) |
| Description | Oracle has released security updates addressing multiple vulnerabilities that exist in third party products which affect Oracle Solaris. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>Oracle advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Oracle Solaris 11.4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.oracle.com/security-alerts/bulletinapr2025.html |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | SUSE has released security updates addressing multiple vulnerabilities that exist in SUSE Linux Kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>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<br>SUSE Enterprise Storage 7.1<br>SUSE Linux Enterprise High Availability Extension 15 SP3, 15 SP4<br>SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5<br>SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4, 15 SP5<br>SUSE Linux Enterprise High Performance Computing LTSS 15 SP3, 15 SP4, 15 SP5<br>SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5<br>SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5<br>SUSE Linux Enterprise Micro for Rancher 5.2, 5.3, 5.4<br>SUSE Linux Enterprise Real Time 15 SP4, SP5<br>SUSE Linux Enterprise Server 15 SP3, SP4, SP5<br>SUSE Linux Enterprise Server 15 SP3 Business Critical Linux<br>SUSE Linux Enterprise Server 15 SP3 LTSS, SP4 LTSS, SP5 LTSS<br>SUSE Linux Enterprise Server for SAP Applications 15 SP3, SP4, SP5<br>SUSE Manager Proxy 4.2, 4.3<br>SUSE Manager Retail Branch Server 4.2, 4.3<br>SUSE Manager Server 4.2, 4.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2025/suse-su-202501640-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202501633-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202501627-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202501620-1/ |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-20242, CVE-2025-20112, CVE-2025-20267, CVE-2025-20257, CVE-2025-20256, CVE-2025-20113, CVE-2025-20114, CVE-2025-20152) |
| Description | Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Privilege Escalation, Cross-Site Scripting, Denial of Service and read or modification of data.<br>Cisco advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | • Cisco Unified CCE Cloud Connect Release 12.6.2<br>• Cisco ISE Software Releases 3.4, 3.3, 3.2, 3.1 and earlier<br>• Cisco Secure Network Analytics Releases 7.5.2, 7.5.1, 7.5.0, 7.4.2<br>• Cisco Unified Intelligence Center Releases 12.5 and 12.6<br>• Cisco Unified CCX Release 12.5(1)SU3 and earlier<br>• Cisco ISE Release 3.4 if it is configured with RADIUS authentication services.<br>• Following Unified Communications Products if they are running on Cisco Software Releases 12.5, 14 and 15<br>Emergency Responder<br>Prime Collaboration Deployment<br>Unified CM<br>Unified CM SME<br>Unified IM&P<br>Unity Connection<br>• Following Contact Center Solutions Products if they are running on Cisco Software Release 12<br>Customer Collaboration Platform<br>Finesse<br>Unified Intelligence Center<br>Virtualized Voice Browser |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-contcent-insuffacces-ArDOVhN8<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-kkhZbHR5<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stored-xss-Yff54m73<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-apiacv-4B6X5ysw<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sna-ssti-dPuLqSmZ<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuis-priv-esc-3Pk96SU4<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-restart-ss-uf986G2Q |

| | |
|---|---|
| Affected Product | **Oracle** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-47538, CVE-2024-47606, CVE-2025-1244, CVE-2025-3028, CVE-2024-47537, CVE-2025-27830, CVE-2020-10713, CVE-2022-2601, CVE-2024-56171, CVE-2025-26594, CVE-2023-40547, CVE-2024-53580, CVE-2024-55605, CVE-2022-48622, CVE-2022-28737, CVE-2023-45322, CVE-2025-1938, CVE-2025-25186, CVE-2017-10176, CVE-2024-25062, CVE-2024-50602, CVE-2025-22871, CVE-2025-27219, CVE-2024-56826, CVE-2024-11079, CVE-2024-34459, CVE-2024-50612, CVE-2025-1492, CVE-2023-4692, CVE-2024-12133, CVE-2024-52615, CVE-2024-52616, CVE-2025-26699, CVE-2024-56378, CVE-2024-50349, CVE-2024-11053, CVE-2024-57970, CVE-2024-46901) |
| Description | Oracle has released security updates addressing multiple vulnerabilities that exist in third party products which affect Oracle Solaris. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>Oracle advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Oracle Solaris 11.4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.oracle.com/security-alerts/bulletinapr2025.html |

| | |
|---|---|
| Affected Product | **cPanel** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-23166, CVE-2025-23165, CVE-2025-23167) |
| Description | cPanel has released security updates for EasyApache 4 addressing multiple vulnerabilities in NodeJS 20 and NodeJS 22. These vulnerabilities could be exploited by malicious users to compromise the affected system.<br>cPanel advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | EasyApache 4 versions prior to 25.16 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://news.cpanel.com/easyapache4-v25-16-maintenance-and-security-release/ |

| | |
|---|---|
| Affected Product | **F5** |
| Severity | **Medium** |
| Affected Vulnerability | Denial of Service Vulnerability (CVE-2024-24983) |
| Description | F5 has released security updates addressing a Denial of Service Vulnerability that exists in Intel Ethernet Controllers and Adapters that affects rSeries appliances.<br>**CVE-2024-24983** - Protection mechanism failure in firmware for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 4.4 may allow an unauthenticated user to potentially enable denial of service via network access.<br>F5 advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | All variants of r2000 series and r4000 series appliances which are running on F5OS-A versions 1.8.0 and 1.5.1 - 1.5.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://my.f5.com/manage/s/article/K000151431 |

| | |
|---|---|
| Affected Product | **Drupal** |
| Severity | **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-48444, CVE-2025-48013, CVE-2025-48445, CVE-2025-48446, CVE-2025-48448, CVE-2025-48447) |
| 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, Denial of Service and Cross Site Scripting.<br>Drupal advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Quick Node Block versions prior to 2.0.0<br>Commerce Eurobank (Redirect) versions prior to 2.1.1 for Drupal 8.x<br>Commerce Alphabank Redirect versions prior to 1.0.3 for Drupal 8.x<br>Admin Audit Trail versions prior to 1.0.5 for Drupal 9/10/11<br>Lightgallery versions prior to 1.6.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.drupal.org/sa-contrib-2025-064<br>• https://www.drupal.org/sa-contrib-2025-065<br>• https://www.drupal.org/sa-contrib-2025-066<br>• https://www.drupal.org/sa-contrib-2025-067<br>• https://www.drupal.org/sa-contrib-2025-068<br>• https://www.drupal.org/sa-contrib-2025-069 |

**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.**