Advisory Alert

Alert Number: AAA20251205 **Date:** December 5, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium	Multiple Vulnerabilities
WatchGuard	**High**, Medium	Multiple Vulnerabilities
Cisco	Medium	Multiple Vulnerabilities
F5	Medium	Heap Out-of-bound Read Vulnerability
Red Hat	Medium	Multiple Vulnerabilities

Description

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	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP5 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20254320-1/

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-56596, CVE-2023-52975)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-56596** - Fix array-index-out-of-bounds in jfs_readdir The stbl might contain some invalid values. Added a check to return error code in that case. **CVE-2023-52975** - Fix UAF during logout when accessing the shost ipaddress. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7911-1

Affected Product	**Dell**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-40897, CVE-2023-40403, CVE-2023-52968, CVE-2023-52969, CVE-2024-6345, CVE-2025-32023, CVE-2025-32988, CVE-2025-32990, CVE-2025-47273, CVE-2025-48367, CVE-2025-6395, CVE-2025-7424, CVE-2025-27249, CVE-2025-46427, CVE-2025-46428)
Description	Dell 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. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerEdge XE9680 Driver versions prior to 1.21.0 Dell PowerEdge XE7740 Driver versions prior to 1.21.0 Dell Networking OS10 versions prior to 10.5.6.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000399990/dsa-2025-417-dell-poweredge-server-security-update-for-intel-gpu-vulnerability • https://www.dell.com/support/kbdoc/en-us/000399887/dsa-2025-395-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-13986, CVE-2025-13984, CVE-2025-13982)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-13986** - The module does not sufficiently block authentication when the REST/HTTP login route is used. An attacker (or legitimate user) with valid credentials can authenticate using the REST login endpoint (/user/login?_format=json) or other HTTP-based authentication routes, effectively bypassing the module's protection of the UI login page. **CVE-2025-13984** - When installed, the module automatically enables cross-origin resource sharing (CORS) with insecure default settings (Access-Control-Allow-Origin: *), overriding any services.yml CORS configuration. This allows any origin to make cross-origin requests to the site without administrator knowledge or consent. **CVE-2025-13982** - The module doesn't sufficiently protect its confirmation routes from cross-site request forgery (CSRF), allowing the logout confirmation route to be triggered without user interaction. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Disable Login Page versions prior to 1.1.3 Next.js module versions prior to 2.0.1 for Drupal 10 or 11 Next.js module versions prior to 1.6.4. for Drupal 9 (1.x branch) Login Time Restriction versions prior to 1.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-124 • https://www.drupal.org/sa-contrib-2025-122 • https://www.drupal.org/sa-contrib-2025-120

Affected Product	**WatchGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-1545, CVE-2025-13939, CVE-2025-13938, CVE-2025-13937, CVE-2025-13936, CVE-2025-12196, CVE-2025-12195, CVE-2025-11838, CVE-2025-12026, CVE-2025-13940)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Cross-Site-Scripting, Arbitrary Code Execution, Memory Corruption. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS 11.0 up to and including 11.12.4+541730 Fireware OS 12.0 up to and including 12.11.4 Fireware OS 12.5 up to and including 12.5.13 Fireware OS 2025.1 up to and including 2025.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00026 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00025 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00024 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00023 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00022 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00021 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00020 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00019 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00018 • https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00017

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20289, CVE-2025-20303, CVE-2025-20304, CVE-2025-20305)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector. These vulnerabilities could allow an authenticated, remote attacker to either disclose sensitive information or conduct a reflected cross-site scripting (XSS) attack. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE Releases 3.4, 3.3, 3.2, 3.1 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multiple-vulns-O9BESWJH

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Heap Out-of-bound Read Vulnerability (CVE-2019-8457)
Description	F5 has released security updates addressing a Heap Out-of-bound Read Vulnerability that exists in SQLite3 which affects BIG-IP modules. **CVE-2019-8457** - This vulnerability allows a remote, low-privileged user to trigger a heap out-of-bounds read in the rtreenode() function, which causes the system to crash. This issue occurs when the user provides a SQLite file containing a maliciously crafted R-Tree table. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP (all modules) versions 17.1.0 - 17.1.2, 16.1.0 - 16.1.5 and 15.1.0 - 15.1.10 BIG-IQ Centralized Management versions 8.3.0 - 8.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000158050

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3884, CVE-2025-4949)
Description	Red Hat 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. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.4 ELS 7 x86_64 JBoss Enterprise Application Platform 8.0 for RHEL 8 x86_64 and 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:22777 • https://access.redhat.com/errata/RHSA-2025:22775 • https://access.redhat.com/errata/RHSA-2025:22773

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.