Advisory Alert

Alert Number: AAA20251218 **Date:** December 18, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Remote Code Execution Vulnerability
Ivanti	**High**	Security Update
ASUS	**High**	Improper Access Control Vulnerability
Dell	**High**	Uncontrolled Resource Consumption Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
SonicWall	**Medium**	Insufficient Authorization Vulnerability
Drupal	**Low**	Information Disclosure Vulnerability

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-37164)
Description	HPE has released a security update addressing a remote code execution vulnerability that is present in HPE OneView. **CVE-2025-37164:** A potential security vulnerability has been identified in Hewlett Packard Enterprise OneView Software. This vulnerability could be exploited, allowing a remote unauthenticated user to perform remote code execution. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE OneView versions prior to v11.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2024-11597)
Description	Ivanti has released a security update addressing a vulnerability that is present in Ivanti Performance Manager. **CVE-2024-11597:** Ivanti has released updates for Performance Manager which address one high severity vulnerability. Successful exploitation could lead to local privilege escalation. Ivanti advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Performance Manager versions 2023.3, 2024.1 and 2024.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/December-2024-Security-Advisory-Ivanti-Performance-Manager-CVE-2024-11597?language=en_US

Affected Product	**ASUS**
Severity	**High**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2025-11901)
Description	ASUS has released a security update addressing an improper access control vulnerability that exists in their products. **CVE-2025-11901**: For compatibility with PCIe add-on devices, the motherboard initializes the IOMMU's DMA protection only during the BIOS POST (Pre-Boot) phase and does not fully enable it until immediately before handing control to the operating system.During this pre-OS window, full DMA protections are not yet enforced. This condition may allow unintended access to system memory by devices capable of performing DMA operations when they are physically connected to the system. ASUS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	UEFI firmware implementations of motherboards based on the Intel Z490, W480, B460, H410, Z590, B560, H510, Z690, B660, W680, Z790, B760, and W790 series chipsets.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Uncontrolled Resource Consumption Vulnerability (CVE-2025-53506)
Description	Dell has released a security update addressing an uncontrolled resource consumption vulnerability that exists in the third-party component Apache Tomcat which is utilized by Dell OpenManage Server Administrator Managed Node. **CVE-2025-53506:** Dell OpenManage Server Administrator (OMSA) remediation is available for an Apache Tomcat Uncontrolled Resource Consumption Vulnerability that could be exploited by malicious users to compromise the affected system Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell OpenManage Server Administrator Managed Node for Windows versions prior to 11.1.0.1 Dell OpenManage Server Administrator Managed Node for RHEL 8.x versions prior to 11.1.0.1 Dell OpenManage Server Administrator Managed Node for RHEL 9.x versions prior to 11.1.0.1 Dell OpenManage Server Administrator Managed Node for SLES 15 versions prior to 11.1.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000404950/dsa-2025-457-dell-openmanage-server-administrator-omsa-security-update-for-apache-tomcat-uncontrolled-resource-consumption-vulnerability

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39864, CVE-2025-39955, CVE-2025-40186, CVE-2022-48701, CVE-2024-46679, CVE-2025-38729, CVE-2025-38718, CVE-2025-38724, CVE-2025-39697, CVE-2025-39757, CVE-2023-53213, CVE-2023-53178, CVE-2023-53226, CVE-2023-53297, CVE-2025-39825, CVE-2025-39817, CVE-2023-53305, CVE-2022-50367, CVE-2023-53365, CVE-2022-50356, CVE-2023-53354, CVE-2023-53393, CVE-2023-53373, CVE-2022-50386, CVE-2022-50403, CVE-2022-50408, CVE-2022-50410, CVE-2022-50406, CVE-2025-39841, CVE-2025-39883, CVE-2023-53680)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux Server - AUS 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:23450 • https://access.redhat.com/errata/RHSA-2025:23445

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-50253, CVE-2023-53676, CVE-2025-21710, CVE-2025-37916, CVE-2025-38359, CVE-2025-38361, CVE-2025-39788, CVE-2025-39805, CVE-2025-39819, CVE-2025-39859, CVE-2025-39944, CVE-2025-39980, CVE-2025-40001, CVE-2025-40021, CVE-2025-40027, CVE-2025-40030, CVE-2025-40038, CVE-2025-40040, CVE-2025-40048, CVE-2025-40055, CVE-2025-40059, CVE-2025-40064, CVE-2025-40070, CVE-2025-40074, CVE-2025-40075, CVE-2025-40083, CVE-2025-40098, CVE-2025-40105, CVE-2025-40107, CVE-2025-40109, CVE-2025-40110, CVE-2025-40111, CVE-2025-40115, CVE-2025-40116, CVE-2025-40118, CVE-2025-40120, CVE-2025-40121, CVE-2025-40127, CVE-2025-40129, CVE-2025-40139, CVE-2025-40140, CVE-2025-40141, CVE-2025-40149, CVE-2025-40154, CVE-2025-40156, CVE-2025-40157, CVE-2025-40159, CVE-2025-40164, CVE-2025-40168, CVE-2025-40169, CVE-2025-40171, CVE-2025-40172, CVE-2025-40173, CVE-2025-40176, CVE-2025-40180, CVE-2025-40183, CVE-2025-40186, CVE-2025-40188, CVE-2025-40194, CVE-2025-40198, CVE-2025-40200, CVE-2025-40204, CVE-2025-40205, CVE-2025-40206, CVE-2025-40207)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2025/suse-su-20254422-1/

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39718, CVE-2022-50543, CVE-2023-53401, CVE-2023-53539, CVE-2023-53513, CVE-2025-38724, CVE-2025-39825, CVE-2025-39883, CVE-2025-39955, CVE-2025-59375, CVE-2025-5372, CVE-2025-47913, CVE-2025-14687, CVE-2022-25927, CVE-2025-6493)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5.0 to 7.5.0 UP14 IF02 IBM Db2 Intelligence Center versions 1.1.0, 1.1.1 and 1.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7255154 • https://www.ibm.com/support/pages/node/7255160

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Insufficient Authorization Vulnerability (CVE-2025-40602)
Description	SonicWall has released a security update addressing an insufficient authorization vulnerability that exist in their products. **CVE-2025-40602**: A local privilege escalation vulnerability due to insufficient authorization in the SonicWall SMA1000 appliance management console (AMC). SonicWall advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SMA1000: • 12.4.3-03093 (platform-hotfix) and earlier versions. • 12.5.0-02002 (platform-hotfix) and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0019

Affected Product	**Drupal**
Severity	**Low**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2025-14840)
Description	Drupal has released a security update addressing an information disclosure vulnerability that exists in Http Client Manager. **CVE-2025-14840**: Http Client Manager introduces a new Guzzle based plugin which allows you to manage HTTP clients using Guzzle Service Descriptions via YAML, JSON or PHP files, in a simple and efficient way. The modules allows administrators to configure HTTP requests as part of Event Condition Action (ECA) automation. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Http Client Manager versions prior to 9.3.13 Http Client Manager versions from 10.0.0 up to but not including 10.0.2 Http Client Manager versions from 11.0.0 up to but not including 11.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2025-126

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.