Advisory Alert

Alert Number: AAA20250109 **Date:** January 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Stack-based Buffer Overflow Vulnerability
Dell	**High**	Multiple Vulnerabilities
Ivanti	**High**	Stack-based Buffer Overflow Vulnerability
Red Hat	**High**	Denial of Service Vulnerability
SUSE	**High**	Multiple Vulnerabilities
cPanel	**High**	Remote Code Execution Vulnerability
HPE	**High**	Traffic Handling Vulnerability
Palo Alto	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Certificate Validation Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23491, CVE-2023-37920, CVE-2023-43804, CVE-2023-45803, CVE-2024-3651 CVE-2024-9287,CVE-2023-50782,CVE-2024-28168,CVE-2024-9681,CVE-2024-21208,CVE-2024-21210,CVE-2024-21217,CVE-2024-21235,CVE-2024-43398,CVE-2024-41123,CVE-2024-41946,CVE-2024-35176,CVE-2024-39908,CVE-2024-10976,CVE-2024-10977,CVE-2024-10978,CVE-2024-10979,CVE-2023-5388,CVE-2024-52533,CVE-2024-43854,CVE-2024-49925,CVE-2024-49945,CVE-2024-50208,CVE-2022-48879,CVE-2022-48956,CVE-2022-48959,CVE-2022-48960,CVE-2022-48962,CVE-2022-48991,CVE-2022-49015,CVE-2024-45013,CVE-2024-45016,CVE-2024-45026,CVE-2024-46716,CVE-2024-46813,CVE-2024-46814,CVE-2024-46815,CVE-2024-46816,CVE-2024-46817,CVE-2024-46818,CVE-2024-46849,CVE-2024-47668,CVE-2024-47674,CVE-2024-47684,CVE-2024-47706,CVE-2024-47747,CVE-2024-47748,CVE-2024-49860,CVE-2024-49930,CVE-2024-49936,CVE-2024-49960,CVE-2024-49969,CVE-2024-49974,CVE-2024-49991,CVE-2024-49995,CVE-2024-50047,CVE-2024-52316, CVE-2025-21111)
Description	Dell has released security updates to address multiple vulnerabilities in their products. If exploited, these vulnerabilities could allow malicious users to compromise the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell VxRail Appliance Versions 8.0.000 through 8.0.311
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000269958/dsa-2025-025-security-update-for-dell-vxrail-for-multiple-vulnerabilities

Affected Product	**Ivanti**
Severity	**Critical**
Affected Vulnerability	Stack-based Buffer Overflow Vulnerability (CVE-2025-0282)
Description	Ivanti has released security updates to address a Stack-based Buffer Overflow Vulnerability affecting Ivanti Connect Secure, Policy Secure, and Neurons for ZTA gateways. If exploited, this vulnerability could allow a remote, unauthenticated attacker to achieve remote code execution. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure: 22.7R2.4 and prior 9.1R18.9 and prior Ivanti Policy Secure 22.7R1 through 22.7R1.2 (Patch planned availability Jan.21) Ivanti Neurons for ZTA gateways 22.7R2 through 22.7R2.3(Patch planned availability Jan.21)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-9287,CVE-2023-50782,CVE-2024-28168,CVE-2024-9681,CVE-2024-21208,CVE-2024-21210,CVE-2024-21217,CVE-2024-21235,CVE-2024-43398,CVE-2024-41123,CVE-2024-41946,CVE-2024-35176,CVE-2024-39908,CVE-2024-10976,CVE-2024-10977,CVE-2024-10978,CVE-2024-10979,CVE-2024-52533,CVE-2024-43854,CVE-2024-49925,CVE-2024-49945,CVE-2024-50208,CVE-2022-48879,CVE-2022-48956,CVE-2022-48959,CVE-2022-48960,CVE-2022-48962,CVE-2022-48991,CVE-2022-49015,CVE-2024-45013,CVE-2024-45016,CVE-2024-45026,CVE-2024-46716,CVE-2024-46813,CVE-2024-46814,CVE-2024-46815,CVE-2024-46816,CVE-2024-46817,CVE-2024-46818,CVE-2024-46849,CVE-2024-47668,CVE-2024-47674,CVE-2024-47684,CVE-2024-47706,CVE-2024-47747,CVE-2024-47748,CVE-2024-49860,CVE-2024-49930,CVE-2024-49936,CVE-2024-49960,CVE-2024-49969,CVE-2024-49974,CVE-2024-49991,CVE-2024-49995,CVE-2024-50047,CVE-2024-52316, CVE-2025-21102)
Description	Dell has released security updates to address multiple vulnerabilities in their products. If exploited, these vulnerabilities could allow malicious users to compromise the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell VxRail Appliance Versions 7.0.000 through 7.0.532
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000269793/dsa-2025-027-security-update-for-dell-vxrail-for-multiple-vulnerabilities

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Stack-based Buffer Overflow Vulnerability (CVE-2025-0283)
Description	Ivanti has released security updates addressing a Stack-based Buffer Overflow Vulnerability affecting Ivanti Connect Secure, Policy Secure, and Neurons for ZTA gateways. This flaw allows a local authenticated attacker to escalate their privileges on the affected device. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure: 22.7R2.4 and prior 9.1R18.9 and prior Ivanti Policy Secure 22.7R1 through 22.7R1.2 (Patch planned availability Jan.21) Ivanti Neurons for ZTA gateways 22.7R2 through 22.7R2.3(Patch planned availability Jan.21)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2024-53122)
Description	Red Hat has released security updates to address a Denial of Service vulnerability in their products, caused by a division-by-zero error in the mptcp_rcv_space_adjust() function within net/mptcp/protocol.c. This issue could allow a remote user to crash the system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:0109

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to use-after-free condition, out of bounds check, out-of-bounds write, null pointer dereference. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 12 SP5 LTSS SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250035-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250034-1/

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Traffic Handling Vulnerability (CVE-2024-54010)
Description	HPE has released a Security update addressing a Traffic Handling Vulnerability for Aruba Networking CX 10000 Series Switches. **CVE-2024-54010 -** A vulnerability in the firewall component of HPE Aruba Networking CX 10000 Series Switches exists. It could allow an unauthenticated adjacent attacker to conduct a packet forwarding attack against the ICMP and UDP protocol. For this attack to be successful an attacker requires a switch configuration that allows packets routing (at layer 3). Configurations that do not allow network traffic routing are not impacted. Successful exploitation could allow an attacker to bypass security policies, potentially leading to unauthorized data exposure. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking CX 10000 Switch Series running the following CX Operating System versions: • AOS-CX 10.15.xxxx: 10.15.0005 and below • AOS-CX 10.14.xxxx: 10.14.1020 and below • AOS-CX 10.13.xxxx: 10.13.1060 and below • AOS-CX 10.10.xxxx: 10.10.1140 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04772en_us&docLocale=en_US

Affected Product	**cPanel**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2024-46981)
Description	cPanel has released security updates to address a Remote Code Execution Vulnerability exists in their products. **CVE-2024-46981** - An authenticated user may use a specially crafted Lua script to manipulate the garbage collector and potentially lead to remote code execution. The problem is fixed in 7.4.2, 7.2.7, and 6.2.17. An additional workaround to mitigate the problem without patching the redis-server executable is to prevent users from executing Lua scripts. This can be done using ACL to restrict EVAL and EVALSHA commands. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All versions of Redis through 6.2.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-1-maintenance-and-security-release/

Affected Product	**Palo Alto**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-0103, CVE-2025-0104, CVE-2025-0105, CVE-2025-0106, CVE-2025-0107)
Description	Palo Alto has released security updates to address multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could allow malicious users to perform SQL injection, reflected cross-site scripting, arbitrary file deletion, file enumeration on the host file system, and OS command injection, potentially leading to the exposure of firewall credentials. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Expedition Migration Tool versions below 1.2.101
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/PAN-SA-2025-0001

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Certificate Validation Vulnerability (CVE-2025-20126)
Description	Cisco has released security updates to address a Certificate Validation Vulnerability that exists in Cisco ThousandEyes Agent. **CVE-2025-20126 -** This vulnerability exists because the affected software does not properly validate certificates for hosted metrics services. An on-path attacker could exploit this vulnerability by intercepting network traffic using a crafted certificate. A successful exploit could allow the attacker to masquerade as a trusted host and monitor or change communications between the remote metrics service and the vulnerable client. Cisco advises to apply security fixes at your earliest to protect systems from potential threats
Affected Products	Cisco ThousandEyes Agent Release macOS versions before 1.206.3 RoomOS versions before 1.207.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thousandeyes-cert-pqtJUv9N

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.