Advisory Alert

Alert Number: AAA20250122 **Date:** January 22, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Oracle	**Critical**	Multiple Vulnerabilities
Ivanti	**Critical**	Stack-based Buffer Overflow Vulnerability
Ivanti	**High**	Stack-based Buffer Overflow Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Node.js	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities
Red hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released its monthly critical security update for January to address multiple vulnerabilities in its products. Exploitation of these vulnerabilities may lead to privilege escalation, denial of service, sensitive information disclosure Oracle advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpujan2025.html

Affected Product	**Ivanti**
Severity	**Critical** - Initial release date 15th January 2025 **(AAA20250115)**
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 through 22.7R2.4 Ivanti Policy Secure 22.7R1 through 22.7R1.2 Ivanti Neurons for ZTA gateways 22.7R2 through 22.7R2.3
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	**Ivanti**
Severity	**High**- Initial release date 15th January 2025 **(AAA20250115)**
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 Ivanti Connect Secure 9.1R18.9 and prior Ivanti Policy Secure 22.7R1 through 22.7R1.2 Ivanti Neurons for ZTA gateways 22.7R2 through 22.7R2.3
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	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-49035, CVE-2023-52524, CVE-2024-53142, CVE-2024-53144, CVE-2024-53146, CVE-2024-53156, CVE-2024-53173, CVE-2024-53179, CVE-2024-53214, CVE-2024-53239, CVE-2024-53240, CVE-2024-56539, CVE-2024-56548, CVE-2024-56604, CVE-2024-56605, CVE-2024-56631, CVE-2024-56704, CVE-2024-8805, CVE-2021-47202, CVE-2024-41087, CVE-2024-50154, CVE-2024-53095, CVE-2024-53206, CVE-2024-53241, CVE-2024-56570, CVE-2024-56598, CVE-2024-56619, CVE-2023-1382, CVE-2023-33951, CVE-2023-33952, CVE-2023-52920, CVE-2024-24860, CVE-2024-26886, CVE-2024-26924, CVE-2024-36915, CVE-2024-42232, CVE-2024-44934, CVE-2024-47666, CVE-2024-47678, CVE-2024-49944, CVE-2024-49952, CVE-2024-50018, CVE-2024-50143, CVE-2024-50166, CVE-2024-50181, CVE-2024-50202, CVE-2024-50211, CVE-2024-50256, CVE-2024-50262, CVE-2024-50278, CVE-2024-50279, CVE-2024-50280, CVE-2024-50296, CVE-2024-53051, CVE-2024-53055, CVE-2024-53056, CVE-2024-53064, CVE-2024-53072, CVE-2024-53090, CVE-2024-53101, CVE-2024-53113, CVE-2024-53114, CVE-2024-53119, CVE-2024-53120, CVE-2024-53122, CVE-2024-53125, CVE-2024-53130, CVE-2024-53131, CVE-2024-53150, CVE-2024-53157, CVE-2024-53158, CVE-2024-53161, CVE-2024-53162, CVE-2024-53210, CVE-2024-53213, CVE-2024-56755)
Description	SUSE has released security updates to address multiple vulnerabilities in their products. Exploiting these vulnerabilities may lead to use-after-free condition, integer overflow, denial of service, out-of-bounds memory access, information disclosure, local privilege escalation SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.3, 15.5 SUSE Linux Enterprise High Availability Extension 15 SP4, 15 SP3, 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP3, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4, 15 SP3, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP3, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.1, 5.2, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4, 5.2 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4, 15 SP3, 15 SP5 SUSE Linux Enterprise Server 15 SP4 LTSS, 15 SP3 LTSS, 15 SP5 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP3, 15 SP5 SUSE Manager Proxy 4.3, 4.2 SUSE Manager Retail Branch Server 4.3, 4.2 SUSE Manager Server 4.3, 4.2 SUSE Enterprise Storage 7.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-20250202-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250203-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-20250201-1/

Affected Product	**Node.js**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23083, CVE-2025-23084, CVE-2025-23085)
Description	Node.js has released its monthly security updates for January to address multiple vulnerabilities in its products. **CVE-2025-23083 -** Worker permission bypass via InternalWorker leak in diagnostics occurs when the diagnostics_channel utility is used to hook into events triggered whenever a worker thread is created. This is not limited to regular workers but also exposes internal workers, allowing their instances to be fetched and their constructors to be obtained and reinstated for malicious purposes. **CVE-2025-23084 -** Path traversal by drive name in Windows environment occurs due to a vulnerability in Node.js that affects the handling of drive names in the Windows environment. Certain Node.js functions fail to treat drive names as special on Windows, causing Node.js to assume the path is relative when it actually refers to the root directory. On Windows, a path that does not start with a file separator is treated as relative to the current directory, and this vulnerability specifically impacts Windows users of the path.join API **CVE-2025-23085-** GOAWAY HTTP/2 frames cause memory leak outside the heap when a remote peer abruptly closes the socket without sending a GOAWAY notification. Furthermore, the same memory leak is triggered if an invalid header is detected by nghttp2, causing the peer to terminate the connection. This flaw can result in increased memory consumption and potentially lead to a denial of service under specific conditions. Node.js advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Node.js versions 23.x, 22.x, 20.x, 18.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/january-2025-security-releases

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53238, CVE-2024-56757)
Description	Ubuntu has released security updates to address multiple vulnerabilities in the Linux kernel for OEM systems. Exploiting these vulnerabilities may lead to a denial of service and system crashes. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7221-1

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-50154, CVE-2024-50275, CVE-2024-53088, CVE-2024-8391, CVE-2024-50379)
Description	Red Hat has released security updates to address multiple vulnerabilities in their products. Exploitation of these vulnerabilities may lead to Denial of service, race condition, remote code execution 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 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 JBoss Enterprise Web Server 6 for RHEL 9 x86_64 JBoss Enterprise Web Server 6 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:0578 • https://access.redhat.com/errata/RHSA-2025:0542 • https://access.redhat.com/errata/RHSA-2025:0343 • https://access.redhat.com/errata/RHSA-2025:0342

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.