TLP: WHITE

Advisory Alert

Alert Number: **AAA20240903** **Date:** **September 3, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Ivanti	**Critical**	Authentication Bypass Vulnerability
SUSE	**High**	Arbitrary Code Execution Vulnerability

Description

Affected Product	**Ivanti**
Severity	**Critical** - Initial release date **14th August 2024 (AAA20240814)**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-7593)
Description	Ivanti has released security updates addressing an Authentication Bypass Vulnerability that exists in their products. The vulnerability is caused due to incorrect implementation of an authentication algorithm in Ivanti vTM other than versions 22.2R1 or 22.7R2, which allows a remote unauthenticated attacker to bypass authentication of the admin panel. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Virtual Traffic Manager - 22.2, 22.3, 22.3R2, 22.5R1, 22.6R1, 22.7R1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Virtual-Traffic-Manager-vTM-CVE-2024-7593?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2023-31315)
Description	SUSE has released security updates addressing an Arbitrary Code Execution Vulnerability that exists in their products. The vulnerability is caused by an improper validation in a model specific register (MSR), which could allow a malicious program with ring0 access to modify SMM configuration. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP5 openSUSE Leap 15.5 openSUSE Leap Micro 5.5 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Performance Computing 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 for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20243081-1/

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.