Advisory Alert

Alert Number: AAA20230728 **Date:** July 28, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Synology	**Critical**	Multiple vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Ivanti	**High**	Privilege Escalation Vulnerability
Ubuntu	**High, Medium, Low**	Multiple Vulnerabilities

Description

Affected Product	**Synology**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Synology has released a security update to address Multiple Vulnerabilities in Synology Mail Station. These vulnerabilities allow remote attackers to potentially inject SQL commands and inject arbitrary web scripts or HTML via a susceptible version of Synology Mail Station Synology highly recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Mail Station for DSM 7.2 Mail Station for DSM 7.1 Mail Station for DSM 7.0 Mail Station for DSM 6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_23_09

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20593 ,CVE-2023-2985 ,CVE-2023-35001)
Description	Suse has released a security updates addressing Multiple Vulnerabilities in their products. if exploited these vulnerabilities could lead to sensitive information disclosure, denial of service and privilege escalation. Suse recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Real Time 12 SP5 SUSE Linux Enterprise Server 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233006-1/

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2023-28129)
Description	Ivanti has released a security update addressing a privilege escalation vulnerability. If exploited, a local low-privileged account user is able to execute arbitrary OS commands as the DSM software installation user, which typically has high privileges. Ivanti recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Ivanti Desktop and Server Management 2022.2 SU2 and all prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA-2023-07-26-CVE-2023-28129?language=en_US

Affected Product	**Ubuntu**
Severity	**High, Medium , Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31248, CVE-2023-3389, CVE-2023-35001, CVE-2023-3141, CVE-2023-3090, CVE-2023-32629, CVE-2023-2640, CVE-2023-3390, CVE-2022-48502)
Description	Ubuntu has released a security update addressing Multiple Vulnerabilities. If exploited, these Vulnerabilities could lead to sensitive information disclosure, privilege escalation, and arbitrary code execution. Ubuntu recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Ubuntu 22.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6260-1

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.