Advisory Alert

Alert Number: **AAA20250919** **Date:** **September 19, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Synology	**Medium**	Security Update

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Real Time Module 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503272-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202502844-2/

Affected Product	**Synology**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-10466)
Description	Synology has released security updates addressing a vulnerability that exists in Safe Access package for SRM. **CVE-2025-10466** - A vulnerability in Safe Access package for SRM allows remote authenticated users with administrator privileges to read or write limited files. Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Safe Access for SRM 1.3 versions prior to 1.3.1-0329
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_25_11

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.