Advisory Alert

Alert Number: AAA20241216 **Date:** December 16, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2024-39008)
Description	IBM has released a security update for Arbitrary Code Execution Vulnerability that exists in their products. **CVE-2024-39008**- robinweser fast-loops could allow a remote attacker to execute arbitrary code on the system, caused by a prototype pollution in the function objectMergeDeep. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar Log Management AQL Plugin version 1.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7178835

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: 15.3, 15.5, 15.6 openSUSE Leap Micro: 5.5 Public Cloud Module: 15-SP6 SUSE Enterprise Storage: 7.1 SUSE Linux Enterprise High Availability Extension: 15 SP3 SUSE Linux Enterprise High Performance Computing: 15 SP3, 15 SP5, LTSS 15 SP3 SUSE Linux Enterprise Live Patching: 15-SP3, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro: 5.1, 5.2, 5.5 SUSE Linux Enterprise Micro for Rancher: 5.2 SUSE Linux Enterprise Real Time: 15 SP5, 15 SP6 SUSE Linux Enterprise Server: 15 SP3, 15 SP3 Business Critical Linux, 15 SP3 LTSS, 15 SP5, 15 SP6 SUSE Linux Enterprise Server for SAP Applications: 15 SP3, 15 SP5, 15 SP6 SUSE Manager: Proxy 4.2, Retail Branch Server 4.2, Server 4.2 SUSE Real Time Module: 15-SP5, 15-SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20244317-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244316-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244315-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244314-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20244313-1/

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.