Advisory Alert

Alert Number: AAA20230320 **Date:** March 20, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**	Arbitrary Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities

Description

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2021-39144)
Description	RedHat has released a security update addressing an Arbitrary code execution vulnerability that exists in Red Hat JBoss Data Grid Text-Only Advisories x86_64 product. **CVE-2021-39144** - A vulnerability that exists because of a flaw that found in xstream, a simple library used to serialize objects to XML and back again. This flaw allows a remote attacker to load and execute arbitrary code from a remote host by manipulating the processed input stream. RedHat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat JBoss Data Grid Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1303

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36280, CVE-2022-38096, CVE-2023-0045, CVE-2023-0461, CVE-2023-0597, CVE-2023-22995, CVE-2023-23559, CVE-2023-26545)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could cause out-of-bounds memory access, integer overflow, null pointer dereference, create a use after free condition and create a double free condition in the net. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Basesystem Module 15-SP4 Development Tools Module 15-SP4 Legacy Module 15-SP4 openSUSE Leap 15.4 openSUSE Leap Micro 5.3 SUSE Linux Enterprise Desktop 15 SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Workstation Extension 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230796-1/

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.