Advisory Alert

Alert Number:	**AAA20240122**	**Date:**	**January 22, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-26555, CVE-2023-51779, CVE-2023-6121, CVE-2023-6531, CVE-2023-6546, CVE-2023-6606, CVE-2023-6610, CVE-2023-6622, CVE-2023-6931, CVE-2023-6932)
Description	SUSE has released security updates addressing multiple vulnerabilities in products. If exploited, these vulnerabilities could lead to escalation of privilege, denial of service, information leak. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.4 openSUSE Leap 15.5 openSUSE Leap Micro 5.3, 5.4 SUSE Linux Enterprise Desktop 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Availability Extension 15 SP4, SP5 SUSE SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3 , 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, SP5 SUSE Linux Enterprise Workstation Extension 15 SP5 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/2024/suse-su-20240156-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240160-1/

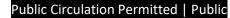|	
Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-22081, CVE-2023-5676)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-22081**- An unspecified vulnerability in Oracle Java SE, Oracle GraalVM for JDK related to the JSSE component could allow a remote attacker to cause low availability impact. **CVE-2023-5676** - Eclipse OpenJ9 is vulnerable to a denial of service, caused by a flaw when a shutdown signal (SIGTERM, SIGINT or SIGHUP) is received before the JVM has finished initializing. By sending a specially crafted request, a local authenticated attacker could exploit this vulnerability to cause an infinite busy hang on a spinlock or a segmentation fault. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
.Affected Products	IBM Db2 10.5.0.x Client and Server IBM Db2 11.1.4.x Client and Server IBM Db2 11.5.x Client and Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7105239

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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)
LankaPay Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka
Hotline: + 94 112039777

Public Circulation Permitted | Public   Report incidents to incident@fincsirt.lk   TLP: WHITE