Advisory Alert

Alert Number: AAA20221114 **Date:** November 14, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Debian	**Critical**	Double-Free Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**, **Medium**	Multiple Vulnerabilities
Debian	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities
Ubuntu	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Debian**
Severity	**Critical**
Affected Vulnerability	Double-Free Vulnerability (CVE-2019-19725)
Description	Debian has released a security update to address a critical vulnerability that exists in the sysstat package that used by the Debian. **CVE-2019-19725** - A double-free vulnerability in check_file_actlst in sa_common.c. was found in sysstat packages through version 12.2.0. A remote attacker could exploit this flaw by creating a specially crafted file with malformed data that, when loaded by a victim, would cause the application to potentially execute arbitrary code. Debian highly recommends to update the sysstat packages at your earliest to avoid issues.
Affected Products	Debian 10 buster versions before 12.0.3-2+deb10u1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security-tracker.debian.org/tracker/CVE-2019-19725

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-45105, CVE-2021-45046, CVE-2021-44228)
Description	IBM has released a security update to address multiple critical vulnerabilities that exists in the IBM DB2 product. **CVE-2021-45105**- Apache Log4j is vulnerable to a denial of service, caused by the failure to protect from uncontrolled recursion from self-referential lookups. A remote attacker can exploit this with a control over Thread Context Map (MDC) input data could craft malicious input data that contains a recursive lookup to cause a StackOverflowError that will terminate the process. **CVE-2021-45046** - Apache Log4j could result in remote code execution, caused by an incomplete fix of CVE-2021-44228 in certain non-default configurations. an attacker with control over Thread Context Map (MDC) input data can craft malicious input data using a JNDI Lookup pattern to leak sensitive information and remote code execution in some environments and local code execution in all environments when the logging configuration uses a non-default Pattern Layout with a Context Lookup **CVE-2021-44228** – Apache Log4j could allow a remote attacker to execute arbitrary code on the system, caused by the failure to protect against attacker controlled LDAP and other JNDI related endpoints by JNDI features. An attacker could exploit this by sending a specially crafted code string, to load arbitrary Java code on the server and take complete control of the system. IBM highly recommends to apply necessary patch updates at your earliest to avoid issues.
Affected Products	Fix pack levels of IBM Db2 V11.5 for all editions on all platforms
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6526462 https://www.ibm.com/support/pages/node/6528672

Affected Product	**SUSE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-33746 CVE-2022-33747 CVE-2022-33748 CVE-2022-42309 CVE-2022-42310 CVE-2022-42311 CVE-2022-42312 CVE-2022-42313 CVE-2022-42314 CVE-2022-42315 CVE-2022-42316 CVE-2022-42317 CVE-2022-42318 CVE-2022-42319 CVE-2022-42320 CVE-2022-42321 CVE-2022-42322 CVE-2022-42323 CVE-2022-42325 CVE-2022-42326, CVE-2021-45710 CVE-2022-24713, CVE-2022-24130, CVE-2017-12852, CVE-2022-1615 CVE-2022-32743, CVE-2022-31628 CVE-2022-31629, CVE-2011-5325 CVE-2015-9261 CVE-2016-2147 CVE-2016-2148 CVE-2016-6301 CVE-2017-15873 CVE-2017-15874 CVE-2017-16544 CVE-2018-1000500 CVE-2018-1000517 CVE-2018-20679 CVE-2019-5747 CVE-2021-28831 CVE-2021-42373 CVE-2021-42374 CVE-2021-42375 CVE-2021-42376 CVE-2021-42377 CVE-2021-42378 CVE-2021-42379 CVE-2021-42380 CVE-2021-42381 CVE-2021-42382 CVE-2021-42383 CVE-2021-42384 CVE-2021-42385 CVE-2021-42386, CVE-2022-42309 CVE-2022-42310 CVE-2022-42311 CVE-2022-42312 CVE-2022-42313 CVE-2022-42314 CVE-2022-42315 CVE-2022-42316 CVE-2022-42317 CVE-2022-42318 CVE-2022-42319 CVE-2022-42320 CVE-2022-42321 CVE-2022-42322 CVE-2022-42323 CVE-2022-42325 CVE-2022-42326)
Description	SUSE has released a security update to address multiple vulnerabilities that exists in their products and packagers that used by their products. Successful exploitation of the most severe vulnerabilities could cause denial of service, arbitrary node creation, unauthorized access to xenstore nodes of deleted nodes, memory corruption, buffer overflow, insecure cookie setup, out of bound read/write and directory traversal. SUSE highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Enterprise Storage 7.1 SUSE Linux Enterprise Desktop 15-SP3 SUSE Linux Enterprise High Performance Computing 15-SP3 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Module for Basesystem 15-SP3 SUSE Linux Enterprise Module for Server Applications 15-SP3 SUSE Linux Enterprise Server 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15-SP3 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2 openSUSE Leap 15.3 openSUSE Leap Micro 5.2 SUSE Linux Enterprise Module for Development Tools 15-SP3 openSUSE Leap 15 SUSE Linux Enterprise Server 12-SP5 SUSE Linux Enterprise Desktop 15-SP4 SUSE Linux Enterprise High Performance Computing 15-SP4 SUSE Linux Enterprise Module for Basesystem 15-SP4 SUSE Linux Enterprise Server 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15-SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 openSUSE Leap 15.4 SUSE Linux Enterprise Server for SAP Applications 12-SP5 SUSE Linux Enterprise Software Development Kit 12-SP5 SUSE Linux Enterprise High Availability 15-SP3 SUSE Linux Enterprise Module for Python2 15-SP3 SUSE Linux Enterprise High Performance Computing 12 SUSE Linux Enterprise Module for Web Scripting 12 SUSE Linux Enterprise Server 12 SUSE Linux Enterprise Server 12-SP3 SUSE Linux Enterprise Server 12-SP4 SUSE Linux Enterprise Server for SAP Applications 12 SUSE Linux Enterprise Server for SAP Applications 12-SP3 SUSE Linux Enterprise Server for SAP Applications 12-SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2022/suse-su-20223947-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223949-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223952-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223953-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223954-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223955-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223957-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223959-1/ https://www.suse.com/support/update/announcement/2022/suse-su-20223960-1/

Affected Product	**Debian**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-36369, CVE-2022-39377, CVE-2019-16167)
Description	Debian has released a security update to address multiple vulnerability that exists in the sysstat package and drop bear SSH server that used by the Debian. **CVE-2021-36369** - Due to a non-RFC-compliant check of the available authentication methods in the client-side SSH code, it is possible for an SSH server to change the login process in its favor. An attacker can use this to bypass additional security measures such as FIDO2 tokens or SSH-Askpass. Thus, it allows an attacker to abuse a forwarded agent for logging on to another server unnoticed. **CVE-2022-39377** – In sysstat versions 9.1.16 and newer but prior to 12.7.1, allocate_structures contains a size_t overflow in sa_common.c. The allocate_structures function insufficiently checks bounds before arithmetic multiplication, allowing for an overflow in the size allocated for the buffer representing system activities. An attacker can use this issue to launch Remote Code Execution attacks. **CVE-2019-16167** – A memory corruption flaw that exists due to an Integer Overflow in remap_struct() in sa_common.c. In the sysstat versions prior to version 12.1.6. Debian highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Debian 10 buster versions before 12.0.3-2+deb10u1 Debian 10 buster versions before 2018.76-5+deb10u2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.debian.org/lts/security/2022/dla-3187 https://www.debian.org/lts/security/2022/dla-3188

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-22390, CVE-2022-22483, CVE-2022-35637, CVE-2021-44832)
Description	IBM has released a security update to address multiple vulnerabilities that exists in the IBM DB2 product. If exploited these vulnerabilities could cause information disclosure, denial of service and arbitrary code execution. IBM highly recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	All fix pack levels of IBM Db2 V9.7, V10.1, V10.5, V11.1, and V11.5 server editions on all platforms
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6597993 https://www.ibm.com/support/pages/node/6618779 https://www.ibm.com/support/pages/node/6618775 https://www.ibm.com/support/pages/node/6549888

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-3266, CVE-2022-40956, CVE-2022-40957, CVE-2022-40958, CVE-2022-40959, CVE-2022-40960, CVE-2022-40962, CVE-2022-39236, CVE-2022-39249, CVE-2022 39250, CVE-2022-39251)
Description	Ubuntu has released a security update addressing multiple vulnerabilities that exist in the thunderbird - Mozilla Open Source mail and newsgroup client and some packages that used by the thunderbird. If exploited these vulnerabilities could cause denial of service, bypass Content Security Policy (CSP) or other security restrictions, execute arbitrary code, sensitive information disclosure or impersonation of another user. Ubuntu highly recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 18.04 LTS Ubuntu 20.04 LTS Ubuntu 22.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5724-1

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.