Advisory Alert

Alert Number: AAA20230411 **Date:** April 11, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0386, CVE-2022-23521, CVE-2022-41903, CVE-2023-0266, CVE-2023-0767)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exist in their kernel and virtualization. **CVE-2023-0386** - The vulnerability exists due to unauthorized access to execution of setuid files in OverlayFS subsystem when copying a capable file from a nosuid mount into another mount. A local user can execute arbitrary code with root privileges. **CVE-2022-23521, CVE-2022-41903, CVE-2023-0266, CVE-2023-0767** – These vulnerabilities exists in the RedHat-Virtualization-Host and redhat-release-virtualization-host packages. if exploited these vulnerabilities can leads to integer overflow, heap buffer overflow, privilege escalation, kernel information leakage and arbitrary memory write. Redhat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization Host 4 for RHEL 8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1681 https://access.redhat.com/errata/RHSA-2023:1677

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-5753, CVE-2021-3923, CVE-2022-20567, CVE-2023-0590, CVE-2023-1076, CVE-2023-1095, CVE-2023-1281, CVE-2023-1390, CVE-2023-1513, CVE-2023-23454, CVE-2023-23455, CVE-2023-28328, CVE-2023-28464, CVE-2023-28772, CVE-2022-4744, CVE-2023-0394, CVE-2023-1582, CVE-2023-1637, CVE-2023-1652, CVE-2023-28327, CVE-2023-28466, CVE-2023-0461, CVE-2023-1075, CVE-2023-1078, CVE-2023-1382, CVE-2023-23004, CVE-2023-25012)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in its products. The exploitation of these vulnerabilities could lead to Information disclosure, Memory leak, Infinite loop, Improper Initialization, Buffer overflow, and use-After-Free condition. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 openSUSE Leap 15.4 Public Cloud Module 15-SP4 SUSE Linux Enterprise High Performance Computing 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 SUSE Enterprise Storage 7 SUSE Linux Enterprise High Availability Extension 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP2 SUSE Manager Proxy 4.1 SUSE Manager Retail Branch Server 4.1 SUSE Manager Server 4.1 SUSE Linux Enterprise High Availability Extension 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20231801-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231802-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231800-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20231803-1/

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.