Advisory Alert

Alert Number: AAA20230913 **Date:** September 13, 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
Lenovo	**High**, Medium	Multiple Vulnerabilities
Microsoft	**High**, Medium	Monthly Security Updates
Ubuntu	Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1637, CVE-2023-3390, CVE-2023-3610, CVE-2023-3776, CVE-2023-4004, CVE-2023-4147, CVE-2023-20593, CVE-2023-21102, CVE-2023-31248, CVE-2023-35001)
Description	RedHat has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Use-after-free condition, Information leakage, Kernel protection bypass, chain binding. RedHat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:5091

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1077, CVE-2023-2176, CVE-2023-3090, CVE-2023-35001, CVE-2023-3567)
Description	Suse has released security updates addressing Linux Kernel Security updates affecting their products. Exploitation of these vulnerabilities could lead to Privilege escalation, Memory corruption, Heap out-of-bounds write, Out-of-boundary read. Suse recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP1 SUSE Linux Enterprise Live Patching 15-SP1 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server for SAP Applications 15 SP1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233582-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233585-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233576-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233566-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233571-1 https://www.suse.com/support/update/announcement/2023/suse-su-20233572-1

Affected Product	**Lenovo**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4606, CVE-2023-4607, CVE-2023-4608, CVE-2022-29470 CVE-2023-3112)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Privilege Escalation and Information Disclosure. Lenovo recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-140960 https://support.lenovo.com/us/en/product_security/LEN-140527 https://support.lenovo.com/us/en/product_security/LEN-128081

Affected Product	**Microsoft**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29332, CVE-2023-33136, CVE-2023-35355, CVE-2023-36736, CVE-2023-36739, CVE-2023-36740, CVE-2023-36742, CVE-2023-36744, CVE-2023-36745, CVE-2023-36756, CVE-2023-36757, CVE-2023-36758, CVE-2023-36759, CVE-2023-36760, CVE-2023-36761, CVE-2023-36762, CVE-2023-36763, CVE-2023-36764, CVE-2023-36765, CVE-2023-36766, CVE-2023-36767, CVE-2023-36770, CVE-2023-36771, CVE-2023-36772, CVE-2023-36773, CVE-2023-36777, CVE-2023-36788, CVE-2023-36792, CVE-2023-36793, CVE-2023-36794, CVE-2023-36796, CVE-2023-36799, CVE-2023-36800, CVE-2023-36801, CVE-2023-36802, CVE-2023-36803, CVE-2023-36804, CVE-2023-36805, CVE-2023-36886, CVE-2023-38139, CVE-2023-38140, CVE-2023-38141, CVE-2023-38142, CVE-2023-38143, CVE-2023-38144, CVE-2023-38146, CVE-2023-38147, CVE-2023-38148, CVE-2023-38149, CVE-2023-38150, CVE-2023-38152, CVE-2023-38155, CVE-2023-38156, CVE-2023-38160, CVE-2023-38161, CVE-2023-38162, CVE-2023-38163, CVE-2023-38164, CVE-2023-41764)
Description	Microsoft has issued the security update for the month of September addressing multiple vulnerabilities that exists in variety of Microsoft products, features, and roles. Updates include defense-in-depth updates to help strengthen security-related aspects, in addition to security improvements for the vulnerabilities. Microsoft strongly advises to apply security fixes at earliest to avoid problems.
Affected Products	Microsoft Identity Linux Broker 3D Viewer Visual Studio Code Microsoft Exchange Server Visual Studio Microsoft Office Word Microsoft Office Outlook Microsoft Office SharePoint Microsoft Office Microsoft Office Excel 3D Builder .NET Framework .NET and Visual Studio .NET Core & Visual Studio Microsoft Dynamics Finance & Operations Windows DHCP Server Microsoft Streaming Service Windows Kernel Windows GDI Windows Scripting Microsoft Dynamics Windows Common Log File System Driver Windows Themes Microsoft Windows Codecs Library Windows Internet Connection Sharing (ICS) Windows TCP/IP Azure HDInsights Windows Defender
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Sep

Affected Product	**Ubuntu**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38429, CVE-2023-38428, CVE-2023-38426, CVE-2022-48425, CVE-2023-2898, CVE-2023-3212, CVE-2023-31084, CVE-2023-21255)
Description	Ubuntu has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of service, Sensitive information disclosure and Arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 22.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6339-3

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.