Advisory Alert

Alert Number: AAA20230315 **Date:** March 15, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Redhat	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1017, CVE-2023-1018, CVE-2023-1213, CVE-2023-1214, CVE-2023-1215, CVE-2023-1216, CVE-2023-1217, CVE-2023-1218, CVE-2023-1219, CVE-2023-1220, CVE-2023-1221, CVE-2023-1222, CVE-2023-1223, CVE-2023-1224, CVE-2023-1228, CVE-2023-1229, CVE-2023-1230, CVE-2023-1231, CVE-2023-1232, CVE-2023-1233, CVE-2023-1234, CVE-2023-1235, CVE-2023-1236, CVE-2023-21708, CVE-2023-22490, CVE-2023-22743, CVE-2023-23383, CVE-2023-23385, CVE-2023-23388, CVE-2023-23389, CVE-2023-23391, CVE-2023-23392, CVE-2023-23393, CVE-2023-23394, CVE-2023-23395, CVE-2023-23396, CVE-2023-23397, CVE-2023-23398, CVE-2023-23399, CVE-2023-23400, CVE-2023-23401, CVE-2023-23402, CVE-2023-23403, CVE-2023-23404, CVE-2023-23405, CVE-2023-23406, CVE-2023-23407, CVE-2023-23408, CVE-2023-23409, CVE-2023-23410, CVE-2023-23411, CVE-2023-23412, CVE-2023-23413, CVE-2023-23414, CVE-2023-23415, CVE-2023-23416, CVE-2023-23417, CVE-2023-23418, CVE-2023-23419, CVE-2023-23420, CVE-2023-23421, CVE-2023-23422, CVE-2023-23423, CVE-2023-23618, CVE-2023-23946, CVE-2023-24856, CVE-2023-24857, CVE-2023-24858, CVE-2023-24861, CVE-2023-24863, CVE-2023-24864, CVE-2023-24865, CVE-2023-24866, CVE-2023-24867, CVE-2023-24868, CVE-2023-24869, CVE-2023-24870, CVE-2023-24871, CVE-2023-24872, CVE-2023-24876, CVE-2023-24879, CVE-2023-24880, CVE-2023-24882, CVE-2023-24890, CVE-2023-24891, CVE-2023-24892, CVE-2023-24906, CVE-2023-24908, CVE-2023-24909, CVE-2023-24910, CVE-2023-24911, CVE-2023-24913, CVE-2023-24919, CVE-2023-24920, CVE-2023-24921, CVE-2023-24922, CVE-2023-24923, CVE-2023-24930)
Description	Microsoft has issued the security update for the month of March 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	Azure Client Server Run-time Subsystem (CSRSS) Internet Control Message Protocol (ICMP) Microsoft Bluetooth Driver Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Office Excel Microsoft Office Outlook Microsoft Office SharePoint Microsoft OneDrive Microsoft PostScript Printer Driver Microsoft Printer Drivers Microsoft Windows Codecs Library Office for Android Remote Access Service Point-to-Point Tunneling Protocol Role: DNS Server Role: Windows Hyper-V Service Fabric Visual Studio Windows Accounts Control Windows Bluetooth Service Windows Central Resource Manager Windows Cryptographic Services Windows Defender Windows HTTP Protocol Stack Windows HTTP.sys Windows Internet Key Exchange (IKE) Protocol Windows Kernel Windows Partition Management Driver Windows Point-to-Point Protocol over Ethernet (PPPoE) Windows Remote Procedure Call Windows Remote Procedure Call Runtime Windows Resilient File System (ReFS) Windows Secure Channel Windows SmartScreen Windows TPM Windows Win32K
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Mar

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-25616, CVE-2023-23857, CVE-2023-27269, CVE-2023-27500, CVE-2023-25617)
Description	SAP has released a security update addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause Arbitrary command execution, Privilege Escalation and System File Over-write. SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SAP Business Objects Business Intelligence Platform (CMC), Versions - 420, 430 SAP NetWeaver AS for Java,Version –7.50 SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions -700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791 SAP NetWeaver AS for ABAP and ABAP Platform (SAPRSBRO Program), Versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757 SAP Business Objects (Adaptive Job Server), Versions - 420, 430
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0683, CVE-2023-25492, CVE-2023-25495, CVE-2022-4568, CVE-2022-3728, CVE-2022-48182, CVE-2022-48183, CVE-2022-4573, CVE-2022-4574, CVE-2022-4575, CVE-2022-48189,)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Privilege Escalation, Unauthorized Access, Arbitrary Code Execution and Denial of Service. Lenovo recommends to apply the necessary patch updates 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-103545 https://support.lenovo.com/us/en/product_security/LEN-106014 https://support.lenovo.com/us/en/product_security/LEN-99936

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0833, CVE-2022-3564, CVE-2022-4269, CVE-2022-4378, CVE-2022-4379, CVE-2023-0179, CVE-2023-0266)
Description	Redhat has released Security Updates addressing Multiple Vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to stack overflow, use-after-free condition, information disclosure and integer overflow. Redhat recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:1241 https://access.redhat.com/errata/RHSA-2023:1202

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-27893, CVE-2023-27501, CVE-2023-26459, CVE-2023-25618, CVE-2023-27498, CVE-2023-26461, CVE-2023-25615, CVE-2023-27270, CVE-2023-27271, CVE-2023-27896, CVE-2023-27894, CVE-2023-26457, CVE-2023-27895, CVE-2023-0021, CVE-2023-27268, CVE-2023-26460, CVE-2023-24526)
Description	SAP has released a security update addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause Arbitrary Code Execution, Directory Traversal, XML external entity (XXE) injection, Cross-site Scripting (XSS). SAP recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SAP ABAP Platform,Versions -751, 753, 753, 754, 756, 757, 791 SAP Authenticator for Android, Version –1.3.0 SAP BusinessObjects Business Intelligence Platform (Web Services), Versions –420, 430 SAP Content Server,Version –7.53 SAP Host Agent, Versions –7.22 SAP NetWeaver Application Server for ABAP and ABAP Platform, Versions -700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791 SAP NetWeaver AS for ABAP and ABAP Platform, Versions -SAP_BASIS 700, 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 791 SAP NetWeaver AS Java (Object Analyzing Service), Versions –7.50 SAP NetWeaver AS Java,Versions–7.50 SAP NetWeaver (SAP Enterprise Portal), Versions –7.50 SAP NetWeaver,Versions–700, 701, 702, 731, 740, 750 SAP Solution Manager and ABAP managed systems (ST-PI), Versions -2008_1_700, 2008_1_710and 740
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://dam.sap.com/mac/app/e/pdf/preview/embed/ucQrx6G?ltr=a&rc=100

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.