Advisory Alert

Alert Number: AAA20230111 **Date:** January 11, 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
Ubuntu	**High**	Denial of service Vulnerability
Debian	**High**	Reflected file download vulnerability
SAP	**Medium**	Multiple vulnerabilities

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-21524,CVE-2023-21525,CVE-2023-21531,CVE-2023-21532,CVE-2023-21535,CVE-2023-21536,CVE-2023-21537,CVE-2023-21539,CVE-2023-21540,CVE-2023-21541 ,CVE-2023-21542,CVE-2023-21543,CVE-2023-21546,CVE-2023-21548,CVE-2023-21549,CVE-2023-21550,CVE-2023-21551,CVE-2023-21552,CVE-2023-21555,CVE-2023-21556,CVE-2023-21557 ,CVE-2023-21558,CVE-2023-21559,CVE-2023-21560,CVE-2023-21561,CVE-2023-21563,CVE-2023-21674 ,CVE-2023-21675,CVE-2023-21676, CVE-2023-21678,CVE-2023-21679,CVE-2023-21680,CVE-2023-21681,CVE-2023-21682,CVE-2023-21724,CVE-2023-21725,CVE-2023-21726,CVE-2023-21730,CVE-2023-21732,CVE-2023-21733,CVE-2023-21734,CVE-2023-21735,CVE-2023-21736,E-2023-21737 ,CVE-2023-21738,CVE-2023-21739,CVE-2023-21741,CVE-2023-21742,CVE-2023-21743,CVE-2023-21744, CVE-2023-21745,CVE-2023-21746,CVE-2023-21747,CVE-2023-21748,CVE-2023-21749,CVE-2023-21750,CVE-2023-21752,CVE-2023-21753,CVE-2023-21754,CVE-2023-21755, CVE-2023-21759 ,CVE-2023-21760,CVE-2023-21761,CVE-2023-21762,CVE-2023-21763,CVE-2023-21764,CVE-2023-21765,CVE-2023-21766,CVE-2023-21767,CVE-2023-21768,CVE-2023-21771,CVE-2023-21772,CVE-2023-21773,CVE-2023-21774,CVE-2023-21776,CVE-2023-21779, CVE-2023-21780,CVE-2023-21781,CVE-2023-21782,CVE-2023-21783,CVE-2023-21784,CVE-2023-21785,CVE-2023-21786,CVE-2023-21787,CVE-2023-21788,CVE-2023-21789,CVE-2023-21790,CVE-2023-21791,CVE-2023-21792,CVE-2023-21793)	
Description	Microsoft has issued the security update for the month of December 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	.NET Core 3D Builder Azure Service Fabric Container Microsoft Bluetooth Driver Microsoft Exchange Server Microsoft Graphics Component Microsoft Local Security Authority Server (lsasrv) Microsoft Message Queuing Microsoft Office Microsoft Office SharePoint Microsoft Office Visio Microsoft WDAC OLE DB provider for SQL Visual Studio Code Windows ALPC Windows Ancillary Function Driver for WinSock Windows Authentication Methods Windows Backup Engine Windows Bind Filter Driver Windows BitLocker Windows Boot Manager Windows Credential Manager Windows Cryptographic Services Windows DWM Core Library Windows Error Reporting Windows Event Tracing Windows IKE Extension Windows Installer	Windows Internet Key Exchange (IKE) Protocol Windows iSCSI Windows Kernel Windows Layer 2 Tunneling Protocol Windows LDAP - Lightweight Directory Access Protocol Windows Local Security Authority (LSA) Windows Local Session Manager (LSM) Windows Malicious Software Removal Tool Windows Management Instrumentation Windows MSCryptDImportKey Windows NTLM Windows ODBC Driver Windows Overlay Filter Windows Point-to-Point Tunneling Protocol Windows Print Spooler Components Windows Remote Access Service L2TP Driver Windows RPC API Windows Secure Socket Tunneling Protocol (SSTP) Windows Smart Card Windows Task Scheduler Windows Virtual Registry Provider Windows Workstation Service
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Jan	

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-0016,CVE-2023-0022, CVE-2022-41272, CVE-2022-41203, CVE-2022-41271,CVE-2023-0017, CVE-2023-0014)
Description	SAP has released a security update addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause SQL injection, Denial of Service and sensitive information disclosure. SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SAP BPC MS 10.0, Versions -800, 810 SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP), Versions -420, 430 SAP NetWeaver Process Integration, Version –7.50 SAP BusinessObjects Business Intelligence Platform (Central Management Console and BI Launchpad), Versions -4.2, 4.3 SAP NetWeaver AS for Java, Version –7.50 SAP NetWeaver ABAP Server and ABAP Platform, Versions-SAP_BASIS 700, 701, 702,710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT
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	**Ubuntu**
Severity	**High**
Affected Vulnerability	Denial of service Vulnerability(CVE-2022-4378)
Description	Ubuntu has released a security update addressing a vulnerability that exists due to a stack overflow flaw that was found in the Linux kernel's SYSCTL subsystem. **CVE-2022-4378-** A vulnerability that exists in the sysctl implementation in the Linux kernel which contained a stack-based buffer overflow. A local attacker could use this to cause a denial of service (system crash) or execute arbitrary code. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	linux-oem-5.17 - Linux kernel for OEM systems linux-oem-6.0 - Linux kernel for OEM systems
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5799-1

Affected Product	**Debian**
Severity	**High**
Affected Vulnerability	Reflected file download vulnerability (CVE-2022-45442)
Description	Debian has released a security update addressing reflected file download vulnerability in their products. **CVE-2022-45442-** A vulnerability exists in the Ruby-Sinatra library, which is used for writing HTTP applications. A Content-Disposition HTTP header was being incorrectly derived from a potentially user-supplied filename. Debian recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	ruby-sinatra (PTS) buster (security) version prior to 2.0.5-4+deb10u2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.debian.org/lts/security/2023/dla-3264

Affected Product	**SAP**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-0012,CVE-2023-0013, CVE-2023-0018, CVE-2023-0015,CVE-2023-2015)
Description	SAP has released a security update addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause Cross-Site Scripting, arbitrary Code Execution and sensitive information disclosure. SAP recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SAP Host Agent (Windows), Versions -7.21, 7.22 SAP NetWeaver AS for ABAP and ABAP Platform,Version–702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757 SAP BusinessObjects Business Intelligence Platform (Central management console), Versions –420, 430 SAP Bank Account Management (Manage Banks), Versions–800,90
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.