Advisory Alert

Alert Number: AAA20230215 **Date:** February 15, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Citrix	**High**	Multiple vulnerabilities
Intel	**High** , **Medium**	Multiple Vulnerabilities
Redhat	**High** , **Medium**	Multiple Vulnerabilities
SAP	**High** , **Medium**	Multiple Vulnerabilities
PHP	**Medium**	Multiple Vulnerabilities
IBM	**Medium** , **Low**	Multiple Vulnerabilities
ManageEngine	**Medium** , **Low**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2019-15126, CVE-2023-21528, CVE-2023-21529, CVE-2023-21553, CVE-2023-21564, CVE-2023-21566, CVE-2023-21567, CVE-2023-21568, CVE-2023-21570, CVE-2023-21571, CVE-2023-21572, CVE-2023-21573, CVE-2023-21684, CVE-2023-21685, CVE-2023-21686, CVE-2023-21687, CVE-2023-21688, CVE-2023-21689, CVE-2023-21690, CVE-2023-21691, CVE-2023-21692, CVE-2023-21693, CVE-2023-21694, CVE-2023-21695, CVE-2023-21697, CVE-2023-21699, CVE-2023-21700, CVE-2023-21703, CVE-2023-21704, CVE-2023-21705, CVE-2023-21706, CVE-2023-21707, CVE-2023-21710, CVE-2023-21713, CVE-2023-21714, CVE-2023-21715, CVE-2023-21716, CVE-2023-21717, CVE-2023-21718, CVE-2023-21720, CVE-2023-21721, CVE-2023-21722, CVE-2023-21777, CVE-2023-21778, CVE-2023-21794, CVE-2023-21797, CVE-2023-21798, CVE-2023-21799, CVE-2023-21800, CVE-2023-21801, CVE-2023-21802, CVE-2023-21803, CVE-2023-21804, CVE-2023-21805, CVE-2023-21806, CVE-2023-21807, CVE-2023-21808, CVE-2023-21809, CVE-2023-21812, CVE-2023-21815, CVE-2023-21817, CVE-2023-21820, CVE-2023-21822, CVE-2023-21823, CVE-2023-23374, CVE-2023-23376, CVE-2023-23377, CVE-2023-23378, CVE-2023-23379, CVE-2023-23381, CVE-2023-23382, CVE-2023-23390)
Description	Microsoft has issued the security update for the month of February 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 and Visual Studio .NET Framework 3D Builder Azure App Service Azure Data Box Gateway Azure DevOps Azure Machine Learning HoloLens Internet Storage Name Service Microsoft Defender for Endpoint Microsoft Defender for IoT Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Graphics Component Microsoft Office Microsoft Office OneNote Microsoft Office Publisher Microsoft Office SharePoint Microsoft Office Word Microsoft PostScript Printer Driver Microsoft WDAC OLE DB provider for SQL Microsoft Windows Codecs Library Power BI SQL Server Visual Studio Windows Active Directory Windows ALPC Windows Common Log File System Driver Windows Cryptographic Services Windows Distributed File System (DFS) Windows Fax and Scan Service Windows HTTP.sys Windows Installer Windows iSCSI Windows Kerberos Windows MSHTML Platform Windows ODBC Driver Windows Protected EAP (PEAP) Windows SChannel Windows Win32K
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Feb

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-24483, CVE-2023-24484, CVE-2023-24485, CVE-2023-24486)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to privilege escalation and Improper Access Control. Citrix recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Citrix Workspace app for Linux before 2302 Citrix Workspace App versions before 2212 Citrix Workspace App 2203 LTSR before CU2 Citrix Workspace App 1912 LTSR before CU7 Hotfix 2 (19.12.7002) Citrix Virtual Apps and Desktops versions before 2212 Citrix Virtual Apps and Desktops 2203 LTSR before CU2 Citrix Virtual Apps and Desktops 1912 LTSR before CU6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-security-bulletin-for-cve202324483 https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve202324484-cve202324485 https://support.citrix.com/article/CTX477618/citrix-workspace-app-for-linux-security-bulletin-for-cve202324486

Affected Product	**Intel**
Severity	**High** , **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-25905, CVE-2022-25987, CVE-2022-25992, CVE-2022-26032, CVE-2022-26052, CVE-2022-26062, CVE-2022-26076, CVE-2022-26345, CVE-2022-26421, CVE-2022-26425, CVE-2022-26512, CVE-2022-26843, CVE-2022-26509, CVE-2022-26841, CVE-2022-21216, CVE-2022-26840, CVE-2022-26888, CVE-2022-32570, CVE-2022-33892, CVE-2022-33902, CVE-2021-0187, CVE-2022-26343, CVE-2022-26837, CVE-2022-30539, CVE-2022-30704, CVE-2022-32231, CVE-2022-36348, CVE-2022-36794, CVE-2022-30339, CVE-2022-30530, CVE-2022-32764, CVE-2022-34153, CVE-2022-36398, CVE-2022-30531, CVE-2022-34849, CVE-2022-34157, CVE-2022-37329, CVE-2022-29514, CVE-2022-30692, CVE-2022-31476, CVE-2022-32971, CVE-2022-33190, CVE-2022-33946, CVE-2022-33964, CVE-2022-34854, CVE-2022-33972, CVE-2022-27170, CVE-2022-34346, CVE-2022-34841, CVE-2022-35883, CVE-2022-36289, CVE-2022-32575, CVE-2022-34843, CVE-2022-34864, CVE-2022-29523, CVE-2022-33196, CVE-2022-36287, CVE-2022-21163, CVE-2022-36797, CVE-2022-36397, CVE-2022-36382, CVE-2022-27808, CVE-2022-27234, CVE-2022-38056, CVE-2022-36369, CVE-2021-33104, CVE-2022-38090, CVE-2022-41314)
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products and tools. If exploited, these vulnerabilities could lead to Escalation of Privilege, Information disclosure and Denial of Service. Intel recommends to apply necessary fixes to avoid issues.
Affected Products	10th Generation Intel Core Processor Family Server 11th Gen Intel Core processor Server, Workstation 11th Generation Intel Core Processor Family Mobile 11th Generation Intel Core Processor Family Desktop 12th Generation Intel Core Processor Family Desktop 2nd Generation Intel Xeon Scalable Processors 2nd Generation Intel Xeon Scalable Processors Server 3rd Generation Intel Xeon Scalable Processors Family Server 9th Generation Intel Core Processor Family Desktop Crypto API Toolkit for Intel SGX before version 2.0 commit ID 91ee496. CVAT software maintained by Intel before version 2.0.1. FCS Server software maintained by Intel before version 1.1.79.3. Intel Atom C53xx Processors Edge & Network Intel Atom P53xx Processors Edge & Network Intel Atom P59xx Processors Edge & Network Intel(R) Battery Life Diagnostic Tool software before version 2.2.0 Intel C++ Compiler Classic before version 2021.6 Intel Celeron Processor Family Intel Celeron Processor J Series Desktop, Mobile Intel Celeron Processor N Series Intel Distribution for Python programming language before version 2022.1 Intel DSA software before version 22.4.26. Intel EMA software before version 1.8.1.0. Intel Ethernet 500 Series Controller drivers for VMWare before version 1.10.0.13. Intel Ethernet Controller Administrative Tools drivers for Windows before version 1.5.0.2. Intel Ethernet Network Controllers and Adapters E810 (Columbiaville) Series before version 1.7.0.8: Intel Ethernet X710 (Fortville) Series Controllers and Adapters before version 9.101: Intel FPGA Add-on for Intel oneAPI Base Toolkit before version 2022.2 Intel FPGA SDK for OpenCL with Intel Quartus Prime Pro Edition software before version 22.1. Intel Integrated Sensor Solution before versions 5.4.2.4579v3, 5.4.1.4479 and 5.0.0.4143. Intel Iris Xe MAX drivers for Windows before version 100.0.5.1474. Intel Media SDK software before version 22.2.2. Intel MPI Library before version 2021.6 for Intel oneAPI HPC Toolkit. Intel OFU software before version 14.1.28. Intel oneAPI Collective Communications Library (oneCCL) before version 2021.6. Intel oneAPI Data Analytics Library before version 2021.5. Intel oneAPI Deep Neural Network (oneDNN) before version 2022.1 Intel oneAPI DPC++/C++ Compiler before version 2022.0 Intel oneAPI Toolkits before version 2022.2. Intel Pentium Gold Processor Family Intel Pentium Processor Silver Series Desktop Intel QAT drivers for Linux to version 4.17 Intel Quartus Prime Pro edition software before version 22.2. Intel Quartus Prime Standard edition software before version 22.1STD. Intel Quartus Prime Pro Edition software before version 21.3. Intel Quartus Prime Standard Edition software before version 21.1 Intel SGX SDK software for Linux before version 2.16.100.1. Intel SGX SDK software for Windows before version 2.15.100.1. Intel SPS firmware before version SPS_E3_06.00.03.300.0. Intel SUR software before version 2.4.8902. Intel Trace Analyzer and Collector before version 2021.6. Intel Trace Analyzer and Collector software before version 2021.5. Intel Xeon D processor 1500 series Server Intel Xeon D processor family Server Intel Xeon E processor family Server Intel Xeon E processor family Workstation Intel Xeon E-2300 processor family Workstation Intel Xeon Platinum P-8124, P-8136 processors Server Intel Xeon Scalable processor family Server Intel Xeon W processor family Intel SPS firmware before version SPS_E5_04.04.04.300.0. Oneapi-cli before version 0.2.0 for Intel oneAPI Toolkits. Open CAS software maintained by Intel before version 22.3.1. QATzip software maintained by Intel before version 1.0.9.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/default.html

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-41946, CVE-2021-0341, CVE-2022-47629)
Description	Redhat has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2022-41946 -** A flaw was found in org.postgresql as a result of using PreparedStatement.setText(int, InputStream) and PreparedStatemet.setBytea(int, InputStream) and PreparedStatemet.setBytea(int, InputStream). It allows a user to create a temporary file that is available to all users, which could lead to unexpected behavior. **CVE-2021-0341-** In verifyHostName of OkHostnameVerifier.java, there is a possible way to accept a certificate for the wrong domain due to improperly used crypto. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. **CVE-2022-47629 -** Libksba library contains a vulnerability that is caused by an integer overflow within the CRL's signature parser. This issue can be exploited remotely for code execution on the target system by passing specially crafted data to the application, for example, a malicious S/MIME attachment Redhat recommends to apply necessary fixes to avoid issues.
Affected Products	Red Hat Virtualization Manager 4.4 x86_64 Red Hat Virtualization 4 for RHEL 8 x86_64 Red Hat Virtualization for IBM Power LE 4 for RHEL 8 ppc64le Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:0759 https://access.redhat.com/errata/RHSA-2023:0756

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-41262, CVE-2022-41264, CVE-2022-41268, CVE-2023-0013, CVE-2023-0019, CVE-2023-0020, CVE-2023-0024, CVE-2023-0025, CVE-2023-23851, CVE-2023-23852, CVE-2023-23853, CVE-2023-23854, CVE-2023-23855, CVE-2023-23856, CVE-2023-23858, CVE-2023-23859, CVE-2023-23860, CVE-2023-24521, CVE-2023-24522, CVE-2023-24523, CVE-2023-24524, CVE-2023-24525, CVE-2023-24528, CVE-2023-24529, CVE-2023-24530, CVE-2023-25614)
Description	SAP has released security updates for February 2023 addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause application compromise, arbitrary read and write, Stack-based buffer overflow, server crash and information disclosure. SAP recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	SAP BASIS, Versions –731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, 791 SAP Business Planning and Consolidation,Versions –200, 300 SAP Business Planning and Consolidation,Versions–SAP_BW 750, 751, 752, 753, 754, 755, 756, 757, DWCORE 200, 300, CPMBPC 810 SAP BusinessObjects Business Intelligence (Web Intelligence UI,Version –430 SAP BusinessObjects Business Intelligence platform (Analysis edition for OLAP), Versions -420, 430 SAP BusinessObjects Business Intelligence platform (CMC), Versions -420, 430 SAP CRM (WebClient UI),Versions –700, 701, 702, 731, 740, 750, 751, 752, WEBCUIF 748, 800, 801, S4FND 102, 103 SAP Fiori apps 1.0 for travel management in SAP ERP (My Travel Requests), Version -600 SAP GRC Process Control application, Versions–GRCFND_A V1200, V8100, GRCPINW V1100_700, V1100_731, V1200_750 SAP Host Agent Service, Versions -7.21, 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, 789, 790 SAP NetWeaver AS ABAP (Business Server Pages application),Version –700, 701, 702, 731, 740, 750, 751, 752, 75C, 75D, 75E, 75F, 75G, 75H SAP NetWeaver AS for ABAP and ABAP Platform,Version–700, 701,702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790 SAP NetWeaver AS for Java (Http Provider Service), Version –7.50 SAP S/4 HANA (Map Treasury Correspondence Format Data),Versions-104, 105 SAP Solution Manager (BSP Application), Version –720
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	**PHP**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-0567, CVE-2023-0568, CVE-2023-0662)
Description	PHP has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to arbitrary code execution, denial of service and authentication bypass. **CVE-2023-0567-** The vulnerability exists due to an error within the Password_verify() function, which always returns true with some hashes. A remote attacker can bypass authentication process and gain unauthorized access to the application. **CVE-2023-0568-** The vulnerability exists due to a boundary error when processing untrusted input in fopen_wrappers.c. A remote attacker can pass a specially crafted filename to the affected application, trigger a one-byte buffer overflow and crash the application or potentially execute arbitrary code. **CVE-2023-0662-** The vulnerability exists due to insufficient validation of user-supplied input when parsing multipart request body. A remote attacker can pass specially crafted input to the application and perform a denial of service attack. PHP recommends to apply necessary fixes to avoid issues.
Affected Products	PHP 8.0 PHP 8.1 PHP 8.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/archive/2023.php#2023-02-14-3

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-22393, CVE-2021-39038, CVE-2018-25031, CVE-2021-46708)
Description	IBM has released security updates addressing multiple WebSphere Server related vulnerabilities. If exploited, these vulnerabilities could allow a remote attacker to hijack the clicking action of the victim. IBM recommends to apply necessary fixes to avoid issues.
Affected Products	IBM CICS TX Advanced 10.1, 11.1 IBM CICS TX Standard 11.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6695807 https://www.ibm.com/support/pages/node/6595099 https://www.ibm.com/support/pages/node/6595193 https://www.ibm.com/support/pages/node/6595171

Affected Product	**ManageEngine**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23073, CVE-2023-23074, CVE-2023-23077, CVE-2023-23078)
Description	ManageEngine has released a security update addressing multiple stored cross site scripting vulnerabilities that exist in their products. **CVE-2023-23073** – A stored cross-site scripting (XSS) vulnerability that exists in the products. This Vulnerability allows any low-privileged user to inject malicious JavaScript when associating a service request from the purchase order details page. The JavaScript is executed when the target user views the Associate Service Requests list view in the Purchase Order details page. **CVE-2023-23074** – A stored cross-site scripting (XSS) vulnerability that exist in the products. This vulnerability allows users with the Admin role to inject a malicious JavaScript under the Advanced Portal configurations. The script is executed when a user views the product tour or the product tour preview. **CVE-2023-23077** – A stored cross-site scripting (XSS) vulnerability that exists in the products that allows users to inject a malicious JavaScript in the Add Release page. The script gets executed when a user views the Release Details page. **CVE-2023-23078** – A stored cross-site scripting (XSS) vulnerability allowed users to inject a malicious JavaScript in the asset details page. The script is executed when a user views the asset page. ManageEngine recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	ServiceDesk Plus version 14103 and below ServiceDesk Plus MSP version 13004 and below AssetExplorer 6986 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.manageengine.com/products/service-desk/CVE-2023-23073.html https://www.manageengine.com/products/service-desk/CVE-2023-23074.html https://www.manageengine.com/products/service-desk/CVE-2023-23077.html https://www.manageengine.com/products/service-desk/CVE-2023-23078.html

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.