Advisory Alert

Alert Number: AAA20230510 **Date:** May 10, 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
Intel	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
HP	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Citrix	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-24881, CVE-2023-24898, CVE-2023-24899, CVE-2023-24900, CVE-2023-24901, CVE-2023-24902, CVE-2023-24903, CVE-2023-24904, CVE-2023-24905, CVE-2023-24932, CVE-2023-24939, CVE-2023-24940, CVE-2023-24941, CVE-2023-24942, CVE-2023-24943, CVE-2023-24944, CVE-2023-24945, CVE-2023-24946, CVE-2023-24947, CVE-2023-24948 CVE-2023-24949, CVE-2023-24950, CVE-2023-24953, CVE-2023-24954, CVE-2023-24955, CVE-2023-28251, CVE-2023-28283, CVE-2023-28290, CVE-2023-29324, CVE-2023-29325, CVE-2023-29333,CVE-2023-29335, CVE-2023-29336, CVE-2023-29338, CVE-2023-29340, CVE-2023-29341, CVE-2023-29343, CVE-2023-29344, CVE-2023-29350, CVE-2023-29354)	
Description	Microsoft has released its May 2023 Security Updates which address multiple vulnerabilities across several of products, Which an attacker could use to gain control of an affected system. Microsoft highly recommends to apply relevant patches at earliest to avoid issues.	
Affected Products	Microsoft Teams Windows SMB Microsoft Graphics Component Windows NTLM Windows NFS Portmapper Windows Win32K Windows Secure Socket Tunneling Protocol (SSTP) Windows Installer Remote Desktop Client Windows Secure Boot Reliable Multicast Transport Driver (RMCAST) Windows Network File System Windows Remote Procedure Call Runtime Microsoft Bluetooth Driver Windows iSCSI Target Service	Windows Backup Engine Windows Kernel Microsoft Office SharePoint Microsoft Office Excel Windows LDAP - Lightweight Directory Access Protocol Windows RDP Client Windows MSHTML Platform Windows OLE Microsoft Office Access Microsoft Office Word Visual Studio Code Microsoft Windows Codecs Library SysInternals Microsoft Office Microsoft Edge (Chromium-based)
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-May	

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-44151,CVE-2021-44152,CVE-2021-44153,CVE-2021-44154,CVE-2021-44155, CVE-2023-28762)
Description	SAP has released a security update addressing multiple critical vulnerabilities in their products. Exploitation of these vulnerabilities could cause session hijacking, privilege escalation, run malicious binary on startup, and attacker to enumerate valid users. SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP 3D Visual Enterprise License Manager, Version –15 SAP BusinessObjects Intelligence Platform, 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	**Intel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-33894, CVE-2022-38087)
Description	Intel has released security updates to address multiple vulnerabilities that exist in their products. **CVE-2022-33894** - Improper input validation in the BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access **CVE-2022-38087** - Exposure of resource to wrong sphere in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access Intel recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	8th Generation Intel Core Processor Family 9th Generation Intel Core Processor Family 7th Generation Intel Core Processor Family 10th Generation Intel Core Processor Family Intel Xeon E Processor Family Intel Xeon Scalable Processor Family Intel Xeon Platinum P-8124, P-8136 processors Intel Xeon D processor Family, Intel Xeon W processor Family
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00807.html

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-26341, CVE-2021-33655, CVE-2022-1462, CVE-2022-1789, CVE-2022-1882, CVE-2022-2196, CVE-2022-2663, CVE-2022-3028, CVE-2022-3435, CVE-2022-3522, CVE-2022-3524, CVE-2022-3566, CVE-2022-3567, CVE-2022-3619, CVE-2022-3623, CVE-2022-3625, CVE-2022-3628, CVE-2022-3640, CVE-2022-3707, CVE-2022-4128, CVE-2022-4129, CVE-2022-20141, CVE-2022-21505, CVE-2022-28388, CVE-2022-33743, CVE-2022-39188, CVE-2022-39189, CVE-2022-41674, CVE-2022-42703, CVE-2022-42720, CVE-2022-42721, CVE-2022-42722, CVE-2022-42896, CVE-2022-43750, CVE-2022-47929, CVE-2023-0394, CVE-2023-0461, CVE-2023-0590, CVE-2023-1195, CVE-2023-1382)
Description	RedHat has released a security update addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could leads to use after free condition, privilege escalation, arbitrary code execution, unauthorized random data read, sensitive data exposure and denial of service RedHat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:2458

Affected Product	**HP**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-46769, CVE-2021-26354, CVE-2021-26371, CVE-2021-26379, CVE-2021-26397, CVE-2021-46763, CVE-2021-46756, CVE-2021-46775, CVE-2022-23818, CVE-2023-20524, CVE-2021-46764, CVE-2023-20520, CVE-2021-26356, CVE-2021-26406, CVE-2021-46762)
Description	HP has released firmware updates addressing multiple vulnerabilities that have been identified in the BIOS firmware of HPE ProLiant servers with certain AMD EPYC processors. HP recommends applying necessary firmware updates at earliest to avoid issues
Affected Products	HPE ProLiant DL385 Gen10 Plus server - Prior to v2.60_08-11-2022 HPE ProLiant DL325 Gen10 Plus server - Prior to v2.60_08-11-2022 HPE ProLiant XL675d Gen10 Plus Server - Prior to v2.60_08-11-2022 HPE ProLiant XL645d Gen10 Plus Server - Prior to v2.60_08-11-2022 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v2.60_08-11-2022 HPE ProLiant DL345 Gen10 Plus server - Prior to v2.60_08-11-2022 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v2.60_08-11-2022 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v2.60_08-11-2022 HPE ProLiant DL365 Gen10 Plus server - Prior to v2.60_08-11-2022
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04471en_us

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36691, CVE-2022-43945, CVE-2023-1611, CVE-2023-1670, CVE-2023-1855, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2124, CVE-2023-2162, CVE-2023-30772, CVE-2022-2196 ,CVE-2023-1838 ,CVE-2023-1872 ,CVE-2023-2008, CVE-2023-2176, CVE-2023-0386, CVE-2023-2019, CVE-2023-2235, CVE-2023-23006)
Description	SUSE has released Security Updates addressing Multiple Linux kernel vulnerabilities. The vulnerabilities that have been addressed in these updates include remote code execution, denial of service, and privilege escalation which attackers could potentially exploit. SUSE recommends to apply necessary security fixes at earliest to avoid issue
Affected Products	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 openSUSE Leap 15.4 SUSE CaaS Platform 4.0 SUSE Linux Enterprise High Availability Extension 15 SP1 SUSE Linux Enterprise High Performance Computing 15 SP1 SUSE Linux Enterprise High Performance Computing 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Live Patching 15-SP1 SUSE Linux Enterprise Server 15 SP1 SUSE Linux Enterprise Server 15 SP1 Business Critical Linux 15-SP1 SUSE Linux Enterprise Server 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Server for SAP Applications 15 SP1 SUSE Manager Proxy 4.0 SUSE Manager Retail Branch Server 4.0 SUSE Manager Server 4.0 Basesystem Module 15-SP4 Development Tools Module 15-SP4 Legacy Module 15-SP4 openSUSE Leap Micro 5.3 SUSE Linux Enterprise Desktop 15 SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro for Rancher 5.3 SUSE Linux Enterprise Micro for Rancher 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Workstation Extension 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP3 SUSE Linux Enterprise High Performance Computing LTSS 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP3 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server 15 SP3 Business Critical Linux 15-SP3 SUSE Linux Enterprise Server 15 SP3 LTSS 15-SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2 SUSE Real Time Module 15-SP3 Public Cloud Module 15-SP4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232151-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232146-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232140-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232148-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232147-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232141-1/

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-30744, CVE-2023-29080, CVE-2022-31596, CVE-2022-39014, CVE-2023-32111, CVE-2022-41966, CVE-2023-32113, CVE-2023-30743, CVE-2023-30740, CVE-2023-30741, CVE-2023-30742, CVE-2023-31406, CVE-2022-32244, CVE-2023-31407, CVE-2023-29188, CVE-2022-27667, CVE-2023-31404, CVE-2023-28764, CVE-2023-29111, CVE-2023-32112)
Description	SAP has released a security update addressing multiple vulnerabilities in their products. Exploitation of these vulnerabilities could cause improper access control, privilege escalation, information disclosure, memory corruption, denial of service, and cross site scripting. SAP recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP AS NetWeaver JAVA, Versions -SERVERCORE 7.50, J2EE-FRMW 7.50, CORE-TOOLS 7.50 SAP IBP EXCEL ADD-IN, Versions–2211, 2302, 2305 SAP BusinessObjects Intelligence Platform, Versions –430 SAP PowerDesigner (Proxy), Version -16.7 SAP Commerce, Versions–2105, 2205 and 2211 SAP GUI for Windows, Versions-7.70, 8,0 SAP Commerce (Backoffice), Version–2105, 2205 SAPUI5, Versions-SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 20 SAP BusinessObjects Business Intelligence Platform, Versions -420, 430 SAP CRM (WebClient UI), Versions–S4FND 102, S4FND 103, S4FND 104, S4FND 105, S4FND 106, S4FND 107, WEBCUIF 700, WEBCUIF 701, WEBCUIF 731, WEBCUIF 746, WEBCUIF 747, WEBCUIF 748, WEBCUIF 800, WEBCUIF 80, SAPSCORE 129 SAP Business Planning and Consolidation, Versions-740, 750 SAP BusinessObjects Platform, Versions –420, 430 SAP Application Interface Framework (ODATA service),Versions–755, 756 Vendor Master Hierarchy, Versions –SAP_APPL 500, SAP_APPL 600, SAP_APPL 602, SAP_APPL 603, SAP_APPL 604, SAP_APPL 605, SAP_APPL 606, SAP_APPL 616, SAP_APPL 617, SAP_APPL 618, S4CORE 100
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	**Citrix**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-24487, CVE-2023-24488)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Cross site scripting, Arbitrary file read. Citrix recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Citrix ADC and Citrix Gateway 13.1 before 13.1-45.61 Citrix ADC and Citrix Gateway 13.0 before 13.0-90.11 Citrix ADC and Citrix Gateway 12.1 before 12.1-65.35 Citrix ADC 12.1-FIPS before 12.1-55.296 Citrix ADC 12.1-NDcPP before 12.1-55.296
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX477714/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202324487-cve202324488

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.