Advisory Alert

Alert Number: AAA20230809 **Date:** August 9, 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
Dell	**Critical**	Multiple Vulnerabilities
RedHat	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
SAP	**High**, Medium , Low	Multiple Vulnerabilities
Intel	**High**, Medium , Low	Multiple Vulnerabilities
Citrix	Medium	Multiple Vulnerabilities
HPE	Medium , Low	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38178, CVE-2023-35390, CVE-2023-36873, CVE-2023-38180, CVE-2023-36899, CVE-2023-35391, CVE-2023-38176, CVE-2023-36869, CVE-2023-38188, CVE-2023-35393, CVE-2023-35394, CVE-2023-36881, CVE-2023-36877, CVE-2023-38167, CVE-2023-35945, CVE-2023-35389, CVE-2023-38157, CVE-2023-4068, CVE-2023-4072, CVE-2023-4071, CVE-2023-4073, CVE-2023-4075, CVE-2023-4074, CVE-2023-4076, CVE-2023-4077, CVE-2023-4078, CVE-2023-4070, CVE-2023-4069, CVE-2023-38185, CVE-2023-35388, CVE-2023-35368, CVE-2023-38181, CVE-2023-38182, CVE-2023-21709, CVE-2023-36897, CVE-2023-36896, CVE-2023-35371, CVE-2023-36893, CVE-2023-36895, CVE-2023-36891, CVE-2023-36894, CVE-2023-36890, CVE-2023-36892, CVE-2023-35372, CVE-2023-36865, CVE-2023-36866, CVE-2023-29328, CVE-2023-29330, CVE-2023-36882, CVE-2023-20569, CVE-2023-38170, CVE-2023-36876, CVE-2023-36908, CVE-2023-38169, CVE-2023-36898, CVE-2023-35387, CVE-2023-36904, CVE-2023-36900, CVE-2023-36907, CVE-2023-36906, CVE-2023-38175, CVE-2023-35381, CVE-2023-36889, CVE-2023-35384, CVE-2023-35359, CVE-2023-38154, CVE-2023-35382, CVE-2023-35386, CVE-2023-35380, CVE-2023-38184, CVE-2023-36909, CVE-2023-35376, CVE-2023-38172, CVE-2023-35385, CVE-2023-35383, CVE-2023-36913, CVE-2023-35377, CVE-2023-38254, CVE-2023-36911, CVE-2023-36910, CVE-2023-36912, CVE-2023-38186, CVE-2023-35378, CVE-2023-35379, CVE-2023-36914, CVE-2023-36903, CVE-2023-36905)
Description	Microsoft has issued the security update for the month of August 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 .NET Framework ASP.NET and Visual Studio Azure Arc Azure DevOps Azure HDInsights Dynamics Business Central Control Mariner Memory Integrity System Readiness Scan Tool Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Office Microsoft Office Excel Microsoft Office Outlook Microsoft Office SharePoint Microsoft Office Visio Microsoft Teams Microsoft WDAC OLE DB provider for SQL Microsoft Windows Microsoft Windows Codecs Library Reliability Analysis Metrics Calculation Engine Role: Windows Hyper-V SQL Server Tablet Windows User Interface Windows Bluetooth A2DP driver Windows Cloud Files Mini Filter Driver Windows Common Log File System Driver Windows Cryptographic Services Windows Defender Windows Fax and Scan Service Windows Group Policy Windows HTML Platform Windows Kernel Windows LDAP - Lightweight Directory Access Protocol Windows Message Queuing Windows Mobile Device Management Windows Projected File System Windows Reliability Analysis Metrics Calculation Engine Windows Smart Card Windows System Assessment Tool Windows Wireless Wide Area Network Service
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Aug

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-37483, CVE-2023-37484, CVE-2023-36922)
Description	SAP has released a security update addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could leads to OS command injection, Improper Access Control and Information Disclosure. SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SAP PowerDesigner, Version –16.7 SAP ECC and SAP S/4HANA (IS-OIL), Versions -600, 602, 603, 604, 605, 606, 617, 618, 800, 802, 803, 804, 805, 806, 807
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	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32485, CVE-2023-32484, CVE-2023-28078, CVE-2023-32462, CVE-2021-27795, CVE-2022-33185)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to information disclosure ,Denial of Service, OS command injection Dell highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Dell OS10 Networking Switches running 10.5.2.x and above Dell SmartFabric Storage Software version 1.3 and lower Dell Networking Switches running Enterprise SONiC versions 4.1.0, 4.0.5, 3.5.4 and below Dell Connectrix (Brocade)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216587/dsa-2023-283-security-update-for-dell-smartfabric-storage-software-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000216586/dsa-2023-284-security-update-for-dell-emc-enterprise-sonic-os-command-injection-vulnerability-when-using-remote-user-authentication https://www.dell.com/support/kbdoc/en-us/000216584/dsa-2023-124-security-update-for-dell-smartfabric-os10-multiple-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000216569/dsa-2023-296-security-update-for-dell-connectrix-brocade-for-multiple-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3223, CVE-2021-46877, CVE-2023-1436, CVE-2023-1829, CVE-2023-3090, CVE-2023-35788, CVE-2023-2124)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Out-Of-Memory Error, Denial Of service, out-of-bounds write Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64 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-2023:4516 https://access.redhat.com/errata/RHSA-2023:4515 https://access.redhat.com/errata/RHSA-2023:4509

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31041,CVE-2022-40982, CVE-2022-43505, CVE-2023-41804, CVE-2022-38083, CVE-2022-44611, CVE-2023-23908,CVE-2023-39249)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party components affecting their products. Successful exploitation of these vulnerabilities could lead to Privilege Escalation, Information Disclosure, Denial of Service Dell recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	PowerEdge R660 PowerEdge R760 PowerEdge C6620 PowerEdge MX760c PowerEdge R860 PowerEdge R960 PowerEdge HS5610 PowerEdge HS5620 PowerEdge R660xs PowerEdge R760xs PowerEdge R760xd2 PowerEdge T560 PowerEdge R760xa PowerEdge XE9680 PowerEdge XR5610 PowerEdge XR8620t PowerEdge XR7620 PowerEdge XE8640 PowerEdge R650 PowerEdge R750 PowerEdge R750XA PowerEdge C6520 PowerEdge MX750C PowerEdge R550 PowerEdge R450 PowerEdge R650XS PowerEdge R750XS PowerEdge T550 PowerEdge XR11 PowerEdge XR12 PowerEdge T150 PowerEdge T350 PowerEdge R250 PowerEdge R350 PowerEdge XR4510c PowerEdge XR4520c PowerEdge R740 PowerEdge R740XD PowerEdge R640 PowerEdge R940 PowerEdge R540 PowerEdge R440 PowerEdge T440 PowerEdge XR2 PowerEdge R740XD2 PowerEdge R840 PowerEdge R940XA PowerEdge T640 PowerEdge C6420 PowerEdge FC640 PowerEdge M640 PowerEdge M640 (for PE VRTX) PowerEdge MX740C PowerEdge MX840C PowerEdge C4140 DSS 8440 PowerEdge XE2420 PowerEdge XE7420 PowerEdge XE7440 PowerEdge T140 PowerEdge T340 PowerEdge R240 PowerEdge R340 PowerEdge T130 PowerEdge R230 PowerEdge T330 PowerEdge R330 Dell EMC Storage NX3240 Dell EMC Storage NX3340 Dell EMC NX440 Dell Storage NX430 Dell EMC XC Core XC450 Dell EMC XC Core XC650 Dell EMC XC Core XC750 Dell EMC XC Core XC750xa Dell EMC XC Core XC6520 Dell EMC XC Core 6420 System Dell EMC XC Core XC640 System Dell EMC XC Core XC740xd System Dell EMC XC Core XC740xd2 Dell EMC XC Core XC940 System Dell EMC XC Core XCXR2 Inspiron 5415 SupportAssist for Business PCs
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216589/dsa-2023-178-dell-client-platform-security-update-for-an-insyde-uefi-bios-vulnerability https://www.dell.com/support/kbdoc/en-us/000216580/dsa-2023-206 https://www.dell.com/support/kbdoc/en-us/000216574/security-update-for-dell-supportassist-for-business-pcs-vulnerability

Affected Product	**SAP**
Severity	**High, Medium ,Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39439, CVE-2023-33989, CVE-2023-36923, CVE-2023-39437, CVE-2023-37490, CVE-2023-37491, CVE-2023-33993, CVE-2023-37488, CVE-2023-37486, CVE-2023-39436, CVE-2023-37487, CVE-2023-37492, CVE-2023-39440, CVE-2023-36926)
Description	SAP has released a security update addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Directory Traversal, Improper authentication, Code Injection, Cross-Site Scripting, SQL Injection. SAP recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	SAP Commerce, Versions –HY_COM 2105, HY_COM 2205, COM_CLOUD 2211 SAP NetWeaver (BI CONT ADD ON), Versions –707, 737, 747, 757 SAP PowerDesigner, Version –16.7 SAP Business One, Version –10.0 SAP BusinessObjects Business Intelligence (installer), Versions –420, 430 SAP BusinessObjects Business Intelligence Platform, Versions–420 SAP Message Server, Versions–KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KERNEL 7.77, RNL64UC 7.22, RNL64UC 7.22EXT, RNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22EX SAP Business One (B1i Layer), Version –10.0 SAP Supplier Relationship Management, Versions –600, 602, 603, 604, 605, 606, 616, 617 SAP NetWeaver Process Integration, Versions-SAP_XIESR 7.50, SAP_XITOOL 7.50, SAP_XIAF 7.50 SAP Commerce (OCC API), Versions-HY_COM 2105, HY_COM 2205, COM_CLOUD 2211 SAP Supplier Relationship Management, Versions –600, 602, 603, 604, 605, 606, 616, 617 SAP Business One (Service Layer), Version –10.0 SAP NetWeaver AS ABAP and ABAP Platform, Versions –SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 793, SAP_BASIS 804 SAP BusinessObjects Business Intelligence Platform, Versions–430 SAP Host Agent, Version –7.22
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, Medium ,Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Privilege Escalation, Information Disclosure, Denial of Service Intel recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Multiple products including Firmware, Software and Hardware
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	**Citrix**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34319, CVE-2022-40982, CVE-2023-20569)
Description	Citrix has released a security update addressing multiple vulnerabilities that exist in the Citrix Hypervisor. Successful exploitation of these vulnerabilities could lead to Denial of service and information disclosure. Citrix recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Citrix Hypervisor 8.2 CU1 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX569353/citrix-hypervisor-security-bulletin-for-cve202320569-cve202334319-and-cve202240982

Affected Product	**HPE**
Severity	**Medium , Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	HPE has released security updates addressing multiple third-party vulnerabilities that affect their products. Successful exploitation of these vulnerabilities could lead to Denial of Service, information disclosure, privilege escalation. HPE recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE Servers using certain Intel and AMD Processors HPE Ethernet Adapters, based on the Intel E810 Series Controllers.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/connect/s/securitybulletinlibrary?language=en_US#sort=%40hpescuniversaldate%20descending-&layout=table&numberOfResults=50&f:@kmdoclanguagecode=[cv1871440]&hpe=1

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.