TLP: WHITE

Advisory Alert

Alert Number: AAA20230614 **Date:** June 14, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
VMware	**Low**	Authentication Bypass Vulnerability
Dell	**Low**	Out-of-bounds Write Vulnerability

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-24895, CVE-2023-33126, CVE-2023-24936, CVE-2023-33135, CVE-2023-32032, CVE-2023-32030, CVE-2023-33128, CVE-2023-24897, CVE-2023-29331, CVE-2023-29326, CVE-2023-33141, CVE-2023-21569, CVE-2023-21565, CVE-2023-24896, CVE-2023-2941, CVE-2023-33145, CVE-2023-2937, CVE-2023-2936, CVE-2023-2935, CVE-2023-2940, CVE-2023-2939, CVE-2023-2938, CVE-2023-2931, CVE-2023-2930, CVE-2023-2929, CVE-2023-2934, CVE-2023-2933, CVE-2023-2932, CVE-2023-3079, CVE-2023-29345, CVE-2023-33143, CVE-2023-32031, CVE-2023-28310, CVE-2023-33146, CVE-2023-33133, CVE-2023-32029, CVE-2023-33137, CVE-2023-33140, CVE-2023-33131, CVE-2023-33142, CVE-2023-33129, CVE-2023-33130, CVE-2023-33132, CVE-2023-29357, CVE-2023-32024, CVE-2023-32017, CVE-2023-29372, CVE-2023-29370, CVE-2023-29365, CVE-2023-29337, CVE-2023-29362, CVE-2023-29352, CVE-2023-32020, CVE-2023-29353, CVE-2023-29007, CVE-2023-33139, CVE-2023-25652, CVE-2023-25815, CVE-2023-27911, CVE-2023-27910, CVE-2023-29011, CVE-2023-29012, CVE-2023-27909, CVE-2023-33144, CVE-2023-29364, CVE-2023-32010, CVE-2023-29361, CVE-2023-32009, CVE-2023-32012, CVE-2023-24937, CVE-2023-24938, CVE-2023-29355, CVE-2023-29368, CVE-2023-29358, CVE-2023-29366, CVE-2023-29351, CVE-2023-32018, CVE-2023-32013, CVE-2023-32016, CVE-2023-32011, CVE-2023-32019, CVE-2023-29346, CVE-2023-29373, CVE-2023-29367, CVE-2023-29363, CVE-2023-32014, CVE-2023-32015, CVE-2023-29369, CVE-2023-32008, CVE-2023-32022, CVE-2023-32021, CVE-2023-29360, CVE-2023-29371, CVE-2023-29359)
Description	Microsoft has issued the security update for the month of June 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 Core .NET Framework ASP .NET Azure DevOps Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Office Microsoft Office Excel Microsoft Office OneNote Microsoft Office Outlook Microsoft Office SharePoint Microsoft Power Apps Microsoft Printer Drivers Microsoft WDAC OLE DB provider for SQL Microsoft Windows Codecs Library NuGet Client Remote Desktop Client Role: DNS Server SysInternals Visual Studio Visual Studio Code Windows Authentication Methods Windows Bus Filter Driver Windows Cloud Files Mini Filter Driver Windows Collaborative Translation Framework Windows Container Manager Service Windows CryptoAPI Windows DHCP Server Windows Filtering Windows GDI Windows Geolocation Service Windows Group Policy Windows Hello Windows Hyper-V Windows Installer Windows iSCSI Windows Kernel Windows NTFS Windows ODBC Driver Windows OLE Windows PGM Windows Remote Procedure Call Runtime Windows Resilient File System (ReFS) Windows Server Service Windows SMB Windows TPM Device Driver Windows Win32K
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Jun

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36694, CVE-2022-3566, CVE-2022-4269, CVE-2022-45884, CVE-2022-45885, CVE-2022-45886, CVE-2022-45887, CVE-2022-45919, CVE-2023-1079, CVE-2023-1380, CVE-2023-1382, CVE-2023-1637, CVE-2023-2002, CVE-2023-2124, CVE-2023-2156, CVE-2023-2162, CVE-2023-2176, CVE-2023-2194, CVE-2023-2269, CVE-2023-23586, CVE-2023-2483, CVE-2023-2513, CVE-2023-28410, CVE-2023-28466, CVE-2023-3006, CVE-2023-30456, CVE-2023-31084, CVE-2023-31436, CVE-2023-32233, CVE-2023-32269, CVE-2023-33288)
Description	Suse has released security updates addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause use-after-free condition, out-of-bounds write, out-of-bounds read, and Denial of Service. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4 Public Cloud Module 15-SP4 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 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 12 SP5 SUSE Linux Enterprise Real Time 15 SP3 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3 SUSE Real Time Module 15-SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232500-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232501-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20232502-1/

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3113, CVE-2023-34418, CVE-2023-34420, CVE-2023-34421, CVE-2023-34422, CVE-2023-2992, CVE-2023-2993)
Description	Lenovo has released security updates addressing multiple vulnerabilities in their products. If exploited these vulnerabilities could cause Denial of-service, Privilege Escalation, and Unauthorized Access. Lenovo recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Enclosure - n1200 Enclosure (NeXtScale) Lenovo Fan Power Controller2 (FPC2) Enclosure - n1200 water-cooled Enclosure (NeXtScale) Lenovo Fan Power Controller2 (FPC2) CP-CB-10 (Lenovo) Lenovo System Management Module Firmware v1.24 [TESM34D] CP-CB-10E (Lenovo)Lenovo System Management Module Firmware v1.24 [TESM34D] HX Enclosure Certified Node (ThinkAgile) Lenovo System Management Module Firmware v1.24 [TESM34D] VX Enclosure (ThinkAgile) Lenovo System Management Module Firmware v1.24 [TESM34D] D2 Enclosure (ThinkSystem) Lenovo System Management Module Firmware v1.24 [TESM34D] DA240 Enclosure (ThinkSystem) Lenovo System Management Module 2 Firmware v1.05 [UMSM10P] DW612 Enclosure (ThinkSystem) Lenovo System Management Module 2 Firmware v1.05 [UMSM10P] Lenovo XClarity Administrator (LXCA) Lenovo XClarity Administrator Virtual Appliance Full Image (For KVM) Lenovo XClarity Administrator Virtual Appliance Full Image (For VMWare) Lenovo XClarity Administrator Virtual Appliance Full Image (For Windows)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-98715 https://support.lenovo.com/us/en/product_security/LEN-127357#System%20x

Affected Product	**VMware**
Severity	**Low**
Affected Vulnerability	Authentication Bypass Vulnerability(CVE-2023-20867)
Description	VMware has released a security update addressing Authentication Bypass vulnerability that exists in their VMware Tools. This vulnerability exists due to an error in the vgauth module. An attacker who compromised the ESXi host can bypass authentication process and execute privileged commands. VMware recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	VMware Tools 12.x.x, 11.x.x, 10.3.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0013.html

Affected Product	**Dell**	
Severity	**Low**	
Affected Vulnerability	Out-of-bounds Write Vulnerability (CVE-2023-28064)	
Description	Dell has released a security update addressing Out-of-bounds Write Vulnerability that exists in their products. An unauthenticated physical attacker may potentially exploit this vulnerability, leading to denial of service. Dell recommends to apply the necessary patch updates at your earliest to avoid issues	
Affected Products	Alienware m15 R7 Dell G15 5510 Dell G15 5520 Inspiron 14 5410/5418 Inspiron 15 5510/5518 Inspiron 16 7620 2-in-1 Inspiron 3520 Inspiron 5410 Inspiron 5420 Inspiron 5620 Inspiron 7420 Inspiron 7510 Inspiron 7610 Latitude 3320 Latitude 3420	Latitude 3430 Latitude 3520 Latitude 3530 Precision 5760 Precision 5770 Vostro 3420 Vostro 3520 Vostro 5410 Vostro 5510 Vostro 5620 Vostro 7510 XPS 13 9315 2-in-1 XPS 17 9710 XPS 17 9720
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.dell.com/support/kbdoc/en-us/000214778/dsa-2023-17	

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.