Advisory Alert

Alert Number: AAA20221109 **Date:** November 9, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
VMware	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Multiple Vulnerabilities
Microsoft	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Intel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
RedHat	**Medium**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities
Joomla	**Low**	Reflected Cross Site Scripting Vulnerability

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-39327, CVE-2022-41040, CVE-2022-41080, CVE-2022-38015, CVE-2022-37967, CVE-2022-37966, CVE-2022-41044,CVE-2022-41039, CVE-2022-41088, CVE-2022-41118, CVE-2022-41128)
Description	Microsoft has released security updates for November 2022 addressing multiple critical vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities can lead to code injection, information disclosure, privilege elevation, and Remote code execution. Microsoft highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Azure CLI Microsoft Exchange Server Windows Hyper-V Windows Server Windows 7 Windows RT 8.1 Windows 8.1 Windows 10 Windows 11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-31685, CVE-2022-31686, CVE-2022-31687, CVE-2022-31688, CVE-2022-31689)
Description	VMware has released security updates addressing multiple critical vulnerabilities that exist in the VMware Workspace ONE Assist product. Successful exploitation of the vulnerabilities could leads to authentication bypass, broken authentication, reflected cross site scripting, and session fixation. VMware highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	VMware Workspace ONE Assist versions - 21.x, 22.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0028.html

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27510, CVE-2022-27513, CVE-2022-27516)
Description	Citrix has released a security update addressing multiple critical vulnerabilities that effecting the Citrix ADC and Citrix Gateway. **CVE-2022-27510 –** A vulnerability that exists due to an error in the authentication process when the appliance is configured as VPN (Gateway). A remote non-authenticated attacker can bypass authentication process and gain unauthorized access to Gateway user capabilities. **CVE-2022-27513 –** A vulnerability that exists due to insufficient verification of data authenticity within RDP proxy. A remote attacker can gain control over users' RDP sessions via phishing attack. Successful exploitation of the vulnerability requires the appliance to be configured as VPN (Gateway) and RDP proxy. Also attacker should have initial access to the network via SSL-VPN gateway. **CVE-2022-27516 –** A vulnerability that exists due to incorrect implementation of of the "Max Login Attempts" feature within the VPN (Gateway) and AAA virtual server. An attacker can bypass implemented security restrictions and perform a brute-force attack**.** Citrix highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Citrix ADC and Citrix Gateway 13.1 before 13.1-33.47 Citrix ADC and Citrix Gateway 13.0 before 13.0-88.12 Citrix ADC and Citrix Gateway 12.1 before 12.1.65.21 Citrix ADC 12.1-FIPS before 12.1-55.289 Citrix ADC 12.1-NDcPP before 12.1-55.289
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX463706/citrix-gateway-and-citrix-adc-security-bulletin-for-cve202227510-cve202227513-and-cve202227516

Affected Product	**Microsoft**	
Severity	**High**, **Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41064, CVE-2022-23824, CVE-2022-41085, CVE-2022-41051, CVE-2022-38014, CVE-2022-41066, CVE-2022-41082, CVE-2022-41078, CVE-2022-41079, CVE-2022-41123, CVE-2022-41113, CVE-2022-41052, CVE-2022-41105, CVE-2022-41107, CVE-2022-41104, CVE-2022-41063, CVE-2022-41106, CVE-2022-41122, CVE-2022-41062, CVE-2022-41061, CVE-2022-41060, CVE-2022-41056, CVE-2022-41097, CVE-2022-3786, CVE-2022-3602, CVE-2022-41120, CVE-2022-39253, CVE-2022-41119, CVE-2022-41093, CVE-2022-41045, CVE-2022-41100, CVE-2022-41114, CVE-2022-41099, CVE-2022-41125, CVE-2022-41055, CVE-2022-41095, CVE-2022-41096, CVE-2022-41050, CVE-2022-37992, CVE-2022-41086, CVE-2022-41057, CVE-2022-41053, CVE-2022-41049, CVE-2022-41091, CVE-2022-38023, CVE-2022-41058, CVE-2022-41047, CVE-2022-41048, CVE-2022-41101, CVE-2022-41102, CVE-2022-41116, CVE-2022-41090, CVE-2022-41073, CVE-2022-41054, CVE-2022-41092, CVE-2022-41109, CVE-2022-41098, CVE-2022-41103)	
Description	Microsoft has released security updates for November 2022 addressing multiple vulnerabilities that exist in their products. Successful exploitation of the most severe vulnerabilities can leads to security feature bypass, information disclosure, privilege elevation, Remote code execution, and denial of service. Microsoft highly recommends to apply the necessary security updates at earliest to avoid issues.	
Affected Products	Microsoft .NET Framework Microsoft NuGet Microsoft Windows Server Microsoft Windows RT 8.1 Microsoft Windows 7, 8.1, 10, 11 Azure RTOS GUIX Studio Windows Subsystem for Linux (WSL2) Azure EFLOW Microsoft Dynamics 365 Business Central 2022 Release Wave 1 Microsoft Exchange Server Microsoft Office	Microsoft Office LTSC Microsoft 365 Apps for Enterprise Microsoft Office Web Apps Server Microsoft SharePoint Foundation Microsoft SharePoint Server Microsoft SharePoint Enterprise Server Microsoft Azure Kubernetes Service Azure SDK for C++ and vcpkg Windows Sysmon Microsoft Visual Studio SharePoint Server Subscription Edition Language Pack
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/vulnerability	

Affected Product	**Intel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33064, CVE-2022-26845, CVE-2022-27497, CVE-2022-29893, CVE-2021-33159, CVE-2022-29466, CVE-2022-29515, CVE-2021-26251, CVE-2022-27187, CVE-2022-27233, CVE-2022-30548, CVE-2022-26028, CVE-2022-26341, CVE-2022-26513, CVE-2022-27874, CVE-2022-28611, CVE-2022-26369, CVE-2022-28126, CVE-2022-26367, CVE-2022-26079, CVE-2022-27639, CVE-2022-26045, CVE-2022-28667, CVE-2022-26006, CVE-2022-21198, CVE-2022-26024, CVE-2022-27499, CVE-2022-29486, CVE-2022-26047, CVE-2022-30542, CVE-2021-0185, CVE-2022-25917, CVE-2022-26508, CVE-2022-26086, CVE-2022-33942, CVE-2022-27638, CVE-2022-30297, CVE-2022-33973, CVE-2022-30691, CVE-2022-36367, CVE-2022-36400, CVE-2022-36384, CVE-2022-36380, CVE-2022-36377, CVE-2021-33164, CVE-2022-33176, CVE-2022-37345, CVE-2022-21794, CVE-2022-34152, CVE-2022-32569, CVE-2022-36789, CVE-2022-35276, CVE-2022-38099, CVE-2022-26124, CVE-2022-36370, CVE-2022-37334, CVE-2022-36349)
Description	Intel has released security updates to address multiple vulnerabilities that exist in their products. Exploitation of the most severe vulnerabilities could cause privilege escalation, denial of service, and information disclosure. Intel highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Intel System Studio software all versions. Intel CSME before versions 11.8.93, 11.22.93, 11.12.93, 12.0.92, 14.1.67, 15.0.42, 16.1.25. Intel AMT before versions 11.8.93, 11.22.93, 12.0.92, 14.1.67, 15.0.42, 16.0. Intel SPS before versions SPS_E3_04.01.04.700.0, SPS_E3_06.00.03.035.0. Intel Distribution of OpenVINO Toolkit before version 2021.4.2. Intel Quartus Prime Pro edition software before version 22.1. Intel Glorp gaming particle physics demonstration software version 1.0.0. Intel Quartus Prime Standard edition software before version 21.1 Patch 0.02std. Intel VTune Profiler software before version 2022.2.0. Intel AMT SDK before version 16.0.4.1. Intel EMA before version 1.7.1. Intel MC before version 2.3.2 Intel XMM 7560 Modem M.2 software for Windows or Linux before version M2_7560_R_01.2146.00. Intel Wi-Fi 6E AX411 Intel Wi-Fi 6E AX211 Intel Wi-Fi 6E AX210 Intel Wi-Fi 6 AX201 Intel Wi-Fi 6 AX200 Intel Wireless-AC 9560 Intel Wireless-AC 9462 Intel Wireless-AC 9461 Intel Wireless-AC 9260 Killer Wi-Fi 6E AX1690 Killer Wi-Fi 6E AX1675 Killer Wi-Fi 6 AX1650 Intel Dual Band Wireless-AC 8265 Intel Dual Band Wireless-AC 8260 Intel Dual Band Wireless-AC 3168 Intel Wireless 7265 (Rev D) Family Intel Dual Band Wireless-AC 3165 11th Gen Intel Core processor Intel Xeon W processor 11th Gen Intel Core processor family 12th Generation Intel Core Processor Family Intel NUC 10/11 Performance Mini PC	Intel Pentium Gold Processor Family Intel Celeron Processor Family 10th Generation Intel Core Processor Family Intel Core Processors with Intel Hybrid Technology Intel Pentium Silver N6000 Processor Family, Intel Celeron N4000 and N5000 Processor Families Pentium Gold processor series Celeron processor 5000 series Intel NUC HDMI Firmware Update Tool for NUC7i3DN, NUC7i5DN and NUC7i7DN before version 1.78.2.0.7 Intel SGX SDK software for Linux before version 2.18.100.1. Intel SGX SDK software for Windows before version 2.17.100.1. Hyperscan library maintained by Intel, all versions downloaded before 04/29/2022 Intel Server Board S2600WF Family. Intel Server Board M50CYP Family. Intel Server Board M10JNP Family. Intel Server System R1000WF Family. Intel Server System R2000WF Family. Intel SDP Tool software before version 3.0.0. PresentMon software maintained by Intel before version 1.7.1. Intel DCM software before version 5.0 Intel Advanced Link Analyzer Pro edition software before version 22.2. Intel Advanced Link Analyzer Standard edition software before version 22.1.1 STD. Intel EMA software before version 1.8.0. Intel WAPI Security software for Windows 10/11 before version 22.2150.0.1. Intel Support Android application before version v22.02.28. Intel NUC 8 Rugged Kit - NUC8CCHKR. Intel NUC Kits Intel NUC Board - NUC8CCHB. Intel NUC Mini PC NUC8i7INH and NUC8i5INH. Intel NUC 8 Business and Enthusiast Intel NUC Board Intel NUC M15 Laptop Kit Intel NUC 8 Compute Element Intel NUC 8 Rugged Board NUC 10/11 Performance kit
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	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-36516, CVE-2020-36558, CVE-2021-3640, CVE-2021-30002, CVE-2022-0168, CVE-2022-0617, CVE-2022-0854, CVE-2022-1016, CVE-2022-1048, CVE-2022-1055, CVE-2022-1184, CVE-2022-1852, CVE-2022-2078, CVE-2022-2586, CVE-2022-2639, CVE-2022-2938, CVE-2022-20368, CVE-2022-21499, CVE-2022-26373, CVE-2022-27950, CVE-2022-28390, CVE-2022-28893, CVE-2022-29581, CVE-2022-36946, CVE-2022-24448)
Description	RedHat has released a security update addressing multiple vulnerabilities that exist in their products. Exploitation of the most severe vulnerabilities could leads to exterminating TCP sessions, creating race conditions, kernel pointer leakage, creating a use after free condition, local privilege escalation and denial of service. RedHat highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for Real Time 8 x86_64 Red Hat Enterprise Linux for Real Time for NFV 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:7683 https://access.redhat.com/errata/RHSA-2022:7444

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23816, CVE-2022-23825,CVE-2022-26373,CVE-2022-28693, CVE-2022-29901)
Description	Dell has released Security Updates addressing multiple VMware ESXi vulnerabilities including Return Stack Buffer Underflow, Branch Type Confusion that contains in their products which leads attackers to perform malicious activities. Dell highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Dell EMC VxRail Appliance 4.5.x versions before 4.5.490
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000205143/dsa-2022-292-dell-vxrail-security-update-for-vmware-esxi-vulnerabilities

Affected Product	**Joomla**
Severity	**Low**
Affected Vulnerability	Reflected Cross Site Scripting Vulnerability (CVE-2022-27914)
Description	Joomla has released a security update addressing a reflected cross site scripting vulnerability that exist in the Joomla CMS. Inadequate filtering of potentially malicious user input leads to reflected XSS vulnerabilities in com_media. Joomla recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Joomla CMS versions 4.0.0-4.2.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

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.