Advisory Alert

Alert Number: AAA20221214 **Date:** December 14, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
VMware	**Critical**	Heap Out-of-bounds Write Vulnerability
Citrix	**Critical**	Arbitrary Code Execution Vulnerability
SAP	**Critical**	Multiple Vulnerabilities
SonicWALL	**High**	Arbitrary file deletion vulnerability
Redhat	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**	Multiple Vulnerabilities
OpenSSL	**Low**	Denial of service Vulnerability

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-24480, CVE-2022-26804, CVE-2022-26805, CVE-2022-26806, CVE-2022-41074, CVE-2022-41076, CVE-2022-41077, CVE-2022-41094, CVE-2022-41115, CVE-2022-41121, CVE-2022-41127, CVE-2022-4174, CVE-2022-4175, CVE-2022-4177, CVE-2022-4178, CVE-2022-4179, CVE-2022-4180, CVE-2022-4181, CVE-2022-4182, CVE-2022-4183, CVE-2022-4184, CVE-2022-4185, CVE-2022-4186, CVE-2022-4187, CVE-2022-4188, CVE-2022-4189, CVE-2022-4190, CVE-2022-4191, CVE-2022-4192, CVE-2022-4193, CVE-2022-4194, CVE-2022-4195, CVE-2022-44666, CVE-2022-44667, CVE-2022-44668, CVE-2022-44669, CVE-2022-44670, CVE-2022-44671, CVE-2022-44673, CVE-2022-44674, CVE-2022-44675, CVE-2022-44676, CVE-2022-44677, CVE-2022-44678, CVE-2022-44679, CVE-2022-44680, CVE-2022-44681, CVE-2022-44682, CVE-2022-44683, CVE-2022-44687, CVE-2022-44688, CVE-2022-44689, CVE-2022-44690, CVE-2022-44691, CVE-2022-44692, CVE-2022-44693, CVE-2022-44694, CVE-2022-44695, CVE-2022-44696, CVE-2022-44697, CVE-2022-44698, CVE-2022-44699, CVE-2022-44702, CVE-2022-44704, CVE-2022-44708, CVE-2022-44710, CVE-2022-44713, CVE-2022-47212, CVE-2022-47213)	
Description	Microsoft has issued the security update for the month of December 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 Framework Azure Client Server Run-time Subsystem (CSRSS) Microsoft Bluetooth Driver Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Graphics Component Microsoft Office Microsoft Office OneNote Microsoft Office Outlook Microsoft Office SharePoint Microsoft Office Visio Microsoft Windows Codecs Library Role: Windows Hyper-V SysInternals	Windows Certificates Windows Contacts Windows DirectX Windows Error Reporting Windows Fax Compose Form Windows HTTP Print Provider Windows Kernel Windows PowerShell Windows Print Spooler Components Windows Projected File System Windows Secure Socket Tunneling Protocol (SSTP) Windows SmartScreen Windows Subsystem for Linux Windows Terminal
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2022-Dec	

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Heap Out-of-bounds Write Vulnerability (CVE-2022-31705)
Description	VMware has released a security update to address a Heap out-of-bounds write vulnerability that exists in EHCI controller that is used by the VMware ESXi, Workstation, and Fusion. **CVE-2022-31705** - VMware ESXi, Workstation, and Fusion contain a heap out-of-bounds write vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed. VMware highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	VMware ESXi 8.0, 7.0 VMware Workstation Pro / Player (Workstation) 17.x, 16.x VMware Fusion Pro / Fusion (Fusion) 13.x, 14.x VMware Cloud Foundation 4.x/3.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0033.html

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2022-27518)
Description	Citrix has released a security update addressing an arbitrary code execution vulnerability that exists in Citrix ADC and Citrix Gateway products. **CVE-2022-27518** – A vulnerability that exists in Citrix Gateway and Citrix ADC. An unauthenticated remote attacker can exploit this vulnerability to cause arbitrary code execution on the appliance. Citrix highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Citrix ADC and Citrix Gateway 13.0 before 13.0-58.32 Citrix ADC and Citrix Gateway 12.1 before 12.1-65.25 Citrix ADC 12.1-FIPS before 12.1-55.291 Citrix ADC 12.1-NDcPP before 12.1-55.291
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41267, CVE-2022-41272, CVE-2022-42889, CVE-2022-41271)
Description	SAP has released security updates for December 2022 addressing multiple critical Vulnerabilities that exist in their products. These vulnerabilities includes server side request forgery, Improper access control, and Remote code execution. SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SAP Business Client, Versions - 6.5, 7.0, 7.70 SAP BusinessObjects Business Intelligence Platform,Versions - 420, 430 SAP NetWeaver Process Integration, Version - 7.50 SAP Commerce, Versions-1905, 2005, 2105, 2011, 2205
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	**SonicWALL**
Severity	**High**
Affected Vulnerability	Arbitrary file deletion Vulnerability
Description	SonicWALL has released a security update addressing an arbitrary file deletion vulnerability that exist in Sonicwall Capture Client via SentinelOne Agent. A local attacker with low-privileged access on the target system could escalate privileges and delete files. The exploit was confirmed to work with 6 vulnerable EDR products, including the SentinelOne Agent for Windows. SonicWALL highly recommends to apply necessary fixes at earliest to avoid issues
Affected Products	Versions before SentinelOne Agent for Windows 22.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2022-0025

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1158, CVE-2022-2639,CVE-2022-2601, CVE-2022-3775, CVE-2022-2959, CVE-2022-21123, CVE-2022-21125, CVE-2022-21166, CVE-2022-23816, CVE-2022-23825, CVE-2022-26373, CVE-2022-29900, CVE-2022-29901, CVE-2022-43945, CVE-2022-1292, CVE-2022-2068)
Description	Redhat has released Security Updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of the most severe vulnerabilities could lead to out-of-bounds write access, denial of service, privilege escalation, system crash and arbitrary command execution. Redhat highly recommends to apply necessary security updates at earliest to avoid issues.
Affected Products	JBoss Enterprise Web Server 5 for RHEL 7 x86_64, 8 x86_64, 9 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64, Update Services for SAP Solutions 8.2 x86_64, Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.2 ppc64le, Update Services for SAP Solutions 9.0 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:8989 https://access.redhat.com/errata/RHSA-2022:8978 https://access.redhat.com/errata/RHSA-2022:8973 https://access.redhat.com/errata/RHSA-2022:8974 https://access.redhat.com/errata/RHSA-2022:8913 https://access.redhat.com/errata/RHSA-2022:8917

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-41264, CVE-2022-41268, CVE-2022-39013, CVE-2022-41266, CVE-2022-35737, CVE-2022-41274, CVE-2022-41262, CVE-2022-41275, CVE-2020-6215, CVE-2022-41261, CVE-2022-41215, CVE-2022-41263, CVE-2022-41273)
Description	SAP has released security updates for December 2022 addressing multiple vulnerabilities that exist In their products. Attackers can exploit these vulnerabilities to cause remote code execution, Cross-Site Scripting (XSS), privilege escalation and improper access control. SAP highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	SAP Business Client, Versions -6.5, 7.0, 7.70 SAP Business Objects Business Intelligence Platform (Web intelligence), Versions-420, 430 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 Platform (Program Objects),Versions - 420, 430 SAP BusinessObjects Business Intelligence Platform,Versions - 420, 430 SAP Commerce Webservices 2.0 (Swagger UI), Versions - 1905, 2005, 2105, 2011, 2205 SAP Commerce, Versions -1905, 2005, 2105, 2011, 2205 SAP NetWeaver ABAP Server and ABAP Platform, Versions - 700-702, 731, 740, 750-757, 789, 790 SAP NetWeaver AS ABAP (Business Server Pages Test Application IT00), Versions - 700, 701, 702, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757 SAP NetWeaver AS for Java (Http Provider Service), Version - 7.50 SAP NetWeaver Process Integration,Version - 7.50 SAP Solution Manager (Diagnostic Agent), Version - 7.20 SAP Solution Manager (Enterprise Search), Versions - 740, 750 SAP Sourcing and SAP Contract Lifecycle Management, Version - 1100 SAPBASIS, Versions - 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, 789, 790, 791 SAPUI5 CLIENT RUNTIME, Versions - 600, 700, 800, 900, 1000 SAPUI5, Versions - 754, 755, 756, 757
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	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Denial of service Vulnerability (CVE-2022-3996)
Description	OpenSSL has released Security Updates addressing a denial of service vulnerability that exist in their products. A denial of service vulnerability exist due to a malformed policy constraint. When malformed policy constraint and policy processing is enabled, then a write lock will be taken twice recursively. On some operating systems (most widely: Windows) this results in a denial of service when the affected process hangs. OpenSSL recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	OpenSSL versions 3.0.0 to 3.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20221213.txt

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.