Advisory Alert

Alert Number: AAA20240110 **Date:** January 10, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Privilege Escalation Vulnerabilities
HPE	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Intel	**High**	Multiple Vulnerabilities
FortiGuard	**High**, Medium	Multiple Vulnerabilities
SAP	**High** , Medium , Low	Multiple Vulnerabilities
OpenSSL	**Low**	Denial of service Vulnerability

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0057, CVE-2024-20672, CVE-2024-21312, CVE-2024-20676, CVE-2024-21306, CVE-2024-21325, CVE-2024-0222, CVE-2024-0223, CVE-2024-0224, CVE-2024-0225, CVE-2024-21319, CVE-2024-20677, CVE-2024-21318, CVE-2024-20658, CVE-2024-21307, CVE-2024-0056, CVE-2022-35737, CVE-2024-21305, CVE-2024-20656, CVE-2024-20687, CVE-2024-20674, CVE-2024-20666, CVE-2024-21310, CVE-2024-20694, CVE-2024-20653, CVE-2024-20682, CVE-2024-21311, CVE-2024-20657, CVE-2024-20699, CVE-2024-20700, CVE-2024-20698, CVE-2024-21309, CVE-2024-20697, CVE-2024-20696, CVE-2024-20692, CVE-2024-20660, CVE-2024-20664, CVE-2024-20680, CVE-2024-20663, CVE-2024-21314, CVE-2024-20661, CVE-2024-20690, CVE-2024-20654, CVE-2024-20662, CVE-2024-20655, CVE-2024-20652, CVE-2024-21316, CVE-2024-20681, CVE-2024-21313, CVE-2024-20691, CVE-2024-21320, CVE-2024-20686, CVE-2024-20683)	
Description	Microsoft has issued the security update for the month of January addressing critical multiple vulnerabilities that exists in variety of Microsoft products. Updates include defense-in-depth updates to help strengthen security-related aspects, in addition to security improvements for the vulnerabilities. Microsoft advises to apply security fixes at earliest to avoid problems.	
Affected Products	.NET and Visual Studio .NET Core & Visual Studio .NET Framework Azure Storage Mover Microsoft Bluetooth Driver Microsoft Devices Microsoft Edge (Chromium-based) Microsoft Identity Services Microsoft Office Microsoft Office SharePoint Microsoft Virtual Hard Drive Remote Desktop Client SQL Server SQLite Unified Extensible Firmware Interface Visual Studio Windows AllJoyn API Windows Authentication Methods Windows BitLocker Windows Cloud Files Mini Filter Driver	Windows Collaborative Translation Framework Windows Common Log File System Driver Windows Cryptographic Services Windows Group Policy Windows Hyper-V Windows Kernel Windows Kernel-Mode Drivers Windows Libarchive Windows Local Security Authority Subsystem Service (LSASS) Windows Message Queuing Windows Nearby Sharing Windows ODBC Driver Windows Online Certificate Status Protocol (OCSP) SnapIn Windows Scripting Windows Server Key Distribution Service Windows Subsystem for Linux Windows TCP/IP Windows Themes Windows Win32 Kernel Subsystem Windows Win32K
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Jan	

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Privilege Escalation Vulnerabilities (CVE-2023-49583,CVE-2023-50422,CVE-2023-50423,CVE-2023-50424)
Description	SAP has issued monthly security update addressing Multiple Critical Privilege Escalation vulnerabilities that exists in their products. SAP advises to apply security fixes at earliest to avoid problems.
Affected Products	Applications developed through SAP Business Application Studio, SAP Web IDE Full-Stack and SAP Web IDE for SAP HANA Library-@sap/xssec, Versions before 3.6.0 Library-@sap/approuter, Versions –14.4.2 SAP Edge Integration Cell, Versions after 8.9.13 SAP Business Technology Platform (BTP) Security Services Integration Libraries Library-@sap/xssec, Versions before 3.6.0 Library-cloud-security-services-integration-library, Versions before 2.17.0 & from 3.0.0 before 3.3.0 Library-sap-xssec, Versions before 4.1.0 Library-github.com/sap/cloud-security-client-go, Versions before 0.17.0
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	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-40438, CVE-2023-50274, CVE-2023-50275, CVE-2023-6573)
Description	HPE has issued a security update addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to denial of service, escalation of privilege, server-side request forgery, and remote code execution. HPE advises to apply security fixes at earliest to avoid problems.
Affected Products	HPE OneView All versions prior to 8.70
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04586en_us

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4622,CVE-2023-42753)
Description	Red Hat has released a security update addressing multiple vulnerabilities that exist in their products. Exploiting these vulnerabilities could lead to denial of service, escalation of privileges, and use-after-free issues. **CVE-2023-4622-** A use-after-free flaw in the Linux kernel's af_unix component that allows local privilege escalation. The unix_stream_sendpage() function tries to add data to the last skb in the peer's recv queue without locking the queue. This issue leads to a race condition where the unix_stream_sendpage() function could access a skb that is being released by garbage collection **CVE-2023-42753 -** An array indexing vulnerability in the netfilter subsystem of the Linux kernel. A missing macro could lead to a miscalculation of the h->nets array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0089

Affected Product	**Intel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42429,CVE-2023-38587,CVE-2023-42766,CVE-2023-28738,CVE-2023-28743,CVE-2023-29495,CVE-2023-28722,CVE-2023-32272,CVE-2023-32544,CVE-2023-38541,CVE-2023-29244)
Description	Intel has released security updates addressing multiple vulnerabilities in the Intel NUC firmware and software. If exploited, these vulnerabilities could lead to escalation of privilege and denial of service. Intel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Intel NUC 8 Compute Element Intel NUC 8 Enthusiast Intel NUC Kit Intel NUC 7 Essential Intel NUC Kit Intel NUC 8 Mainstream-G Kit Intel NUC 7 Essential and Intel NUC Kit Intel NUC 9 Pro Compute and Pro Kit Intel NUC Pro Software Suite Configuration Tool before version 3.0.0.6. Intel HotKey Services for Windows 10 for Intel NUC P14E Laptop Element before version 1.1.45. Intel HID Event Filter drivers for Windows 10 for some Intel NUC laptops before version 2.2.2.1. Intel Integrated Sensor Hub (ISH) driver for Windows 10 for Intel NUC P14E Laptop Element before version 5.4.1.4479.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01028.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01009.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00964.html

Affected Product	**FortiGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44250, CVE-2023-46712, CVE-2023-48783)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to Execute unauthorized code or commands, Escalation of privilege and Improper access control. **CVE-2023-44250-** An improper privilege management vulnerability in a FortiOS & FortiProxy HA cluster may allow an authenticated attacker to perform elevated actions via crafted HTTP or HTTPS requests. **CVE-2023-46712-** An improper privilege management vulnerability in FortiPortal may allow a remote and authenticated attacker to add users outside its initial Idp. **CVE-2023-48783**- An Authorization Bypass Through User-Controlled Key vulnerability affecting FortiPortal may allow a remote authenticated user with at least read-only permissions to access to other organization endpoints via crafted GET requests. It is recommended by FortiGuard to apply necessary security fixes at earliest to avoid issues
.Affected Products	FortiOS 7.4.0 through 7.4.1 FortiOS 7.2.5 FortiProxy 7.4.0 through 7.4.1 FortiPortal 6.0 all versions FortiPortal 5.3 all versions FortiPortal version 7.2.0 through 7.2.1 FortiPortal version 7.0.0 through 7.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-315 https://www.fortiguard.com/psirt/FG-IR-23-395 https://www.fortiguard.com/psirt/FG-IR-23-408

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21737, CVE-2023-44487, CVE-2024-22125, CVE-2024-21735, CVE-2024-21736, CVE-2023-31405, CVE-2024-21738, CVE-2024-22124, CVE-2024-21734)
Description	SAP has released a security update addressing multiple vulnerabilities that exist in their products, including code injection, denial of service, improper authorization checks, log injection, cross-site scripting, and information disclosure. It is recommended by SAP to apply necessary security fixes at earliest to avoid issues
Affected Products	SAP Application Interface Framework (File Adapter), Version –702 SAP Web Dispatcher, Versions – WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.85, WEBDISP 7.89, WEBDISP 7.90, WEBDISP 7.94, WEBDISP 7.95, SAP NetWeaver AS ABAP and ABAP Platform, Versions – KRNL64UC 7.53, KERNEL 7.53, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.94, KERNEL 7.93, KERNEL 7.95 Microsoft Edge browser extension (SAP GUI connector for Microsoft Edge), Version -1.0 SAP LT Replication Server, Versions – S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108 SAP S/4HANA Finance (Advanced Payment Management), Version – SAPSCORE 128, S4CORE 10 SAP NetWeaver AS for Java (Log Viewer), Version - ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50 SAP NetWeaver ABAP Application Server and ABAP Platform, Versions – SAP_BASIS 700, SAP_BASIS 701, SAP_BASIS 702, SAP_BASIS 731, SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, 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 79 SAP NetWeaver (Internet Communication Manager), Versions - KERNEL 7.22, KERNEL 7.53, KERNEL 7.54, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KRNL64NUC 7.22, KRNL64NUC 7.22_EXT, WEBDISP 7.22_EXT, WEBDISP 7.53, WEBDISP 7.54 SAP Marketing (Contacts App), Version – 160
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-2023-6129)
Description	OpenSSL has released security updates addressing a denial-of-service vulnerability that exists in their products due to a bug in the POLY1305 MAC (message authentication code) implementation. If exploited, an attacker can corrupt the internal state of applications running on PowerPC CPU-based platforms if the CPU provides vector instructions, which leads to a denial of service. It is recommended by OpenSSL to apply necessary security fixes at earliest to avoid issues
.Affected Products	OpenSSL versions 3.0.0 to 3.0.12 OpenSSL versions 3.1.0 to 3.1.4 OpenSSL versions 3.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20240109.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.