Advisory Alert

Alert Number: AAA20230712 **Date:** July 12, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Remote Code Execution Vulnerability
Fortinet	**Critical**	Stack-Based Overflow Vulnerability
Sap	**Critical**	Command Injection Vulnerability
Suse	**High**	Multiple Vulnerabilities
Redhat	**High**	Multiple Vulnerabilities
Citrix	**High**	Local Privilege escalation Vulnerability
HPE	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities
Sap	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Fortinet	Medium	Insufficient Session Expiration Vulnerability

Description

Affected Product	**Microsoft**	
Severity	**Critical**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-21526, CVE-2023-21756, CVE-2023-29347, CVE-2023-32033, CVE-2023-32034, CVE-2023-32035, CVE-2023-32037, CVE-2023-32038, CVE-2023-32039, CVE-2023-32040, CVE-2023-32041, CVE-2023-32042, CVE-2023-32043, CVE-2023-32044, CVE-2023-32045, CVE-2023-32046, CVE-2023-32047, CVE-2023-32049, CVE-2023-32050, CVE-2023-32051, CVE-2023-32052, CVE-2023-32053, CVE-2023-32054, CVE-2023-32055, CVE-2023-32056, CVE-2023-32057, CVE-2023-32083, CVE-2023-32084, CVE-2023-32085, CVE-2023-33127, CVE-2023-33134, CVE-2023-33148, CVE-2023-33149, CVE-2023-33150, CVE-2023-33151, CVE-2023-33152, CVE-2023-33153, CVE-2023-33154, CVE-2023-33155, CVE-2023-33156, CVE-2023-33157, CVE-2023-33158, CVE-2023-33159, CVE-2023-33160, CVE-2023-33161, CVE-2023-33162, CVE-2023-33163, CVE-2023-33164, CVE-2023-33165, CVE-2023-33166, CVE-2023-33167, CVE-2023-33168, CVE-2023-33169, CVE-2023-33170, CVE-2023-33171, CVE-2023-33172, CVE-2023-33173, CVE-2023-33174, CVE-2023-35296, CVE-2023-35297, CVE-2023-35298, CVE-2023-35299, CVE-2023-35300, CVE-2023-35302, CVE-2023-35303, CVE-2023-35304, CVE-2023-35305, CVE-2023-35306, CVE-2023-35308, CVE-2023-35309, CVE-2023-35310, CVE-2023-35311, CVE-2023-35312, CVE-2023-35313, CVE-2023-35314, CVE-2023-35315, CVE-2023-35316, CVE-2023-35317, CVE-2023-35318, CVE-2023-35319, CVE-2023-35320, CVE-2023-35321, CVE-2023-35322, CVE-2023-35323, CVE-2023-35324, CVE-2023-35325, CVE-2023-35326, CVE-2023-35328, CVE-2023-35329, CVE-2023-35330, CVE-2023-35331, CVE-2023-35332, CVE-2023-35333, CVE-2023-35335, CVE-2023-35336, CVE-2023-35337, CVE-2023-35338, CVE-2023-35339, CVE-2023-35340, CVE-2023-35341, CVE-2023-35342, CVE-2023-35343, CVE-2023-35344, CVE-2023-35345, CVE-2023-35346, CVE-2023-35347, CVE-2023-35348, CVE-2023-35350, CVE-2023-35351, CVE-2023-35352, CVE-2023-35353, CVE-2023-35356, CVE-2023-35357, CVE-2023-35358, CVE-2023-35360, CVE-2023-35361, CVE-2023-35362, CVE-2023-35363, CVE-2023-35364, CVE-2023-35365, CVE-2023-35366, CVE-2023-35367, CVE-2023-35373, CVE-2023-35374, CVE-2023-36867, CVE-2023-36868, CVE-2023-36871, CVE-2023-36872, CVE-2023-36874, CVE-2023-36884)	
Description	Microsoft has issued the security update for the month of July 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 ASP.NET and .NET Azure Active Directory Microsoft Dynamics Microsoft Graphics Component Microsoft Media-Wiki Extensions Microsoft Office Microsoft Office Access Microsoft Office Excel Microsoft Office Outlook Microsoft Office SharePoint Microsoft Power Apps Microsoft Printer Drivers Microsoft Windows Codecs Library Mono Authenticode Paint 3D Role: DNS Server Service Fabric Visual Studio Code Windows Active Directory Certificate Services Windows Active Template Library Windows Admin Center Windows App Store Windows Authentication Methods Windows CDP User Components Windows Certificates Windows Clip Service Windows Cloud Files Mini Filter Driver Windows Cluster Server Windows CNG Key Isolation Service Windows Common Log File System Driver Windows Connected User Experiences and Telemetry Windows CryptoAPI Windows Cryptographic Services Windows Defender	Windows Deployment Services Windows EFI Partition Windows Error Reporting Windows Failover Cluster Windows Geolocation Service Windows HTTP.sys Windows Image Acquisition Windows Installer Windows Kernel Windows Layer 2 Tunneling Protocol Windows Layer-2 Bridge Network Driver Windows Local Security Authority (LSA) Windows Media Windows Message Queuing Windows MSHTML Platform Windows Netlogon Windows Network Load Balancing Windows NT OS Kernel Windows ODBC Driver Windows OLE Windows Online Certificate Status Protocol (OCSP) SnapIn Windows Partition Management Driver Windows Peer Name Resolution Protocol Windows PGM Windows Print Spooler Components Windows Remote Desktop Windows Remote Procedure Call Windows Routing and Remote Access Service (RRAS) Windows Server Update Service Windows SmartScreen Windows SPNEGO Extended Negotiation Windows Transaction Manager Windows Update Orchestrator Service Windows VOLSNAP.SYS Windows Volume Shadow Copy Windows Win32K
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2023-Jul	

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2023-24492)
Description	Citrix has released a security update addressing a Remote Code Execution vulnerability Citrix Secure Access client for Ubuntu. The flaw is exploited when a victim user opens an attacker-crafted link and by accept further prompts Citrix highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Citrix Secure Access client for Ubuntu versions before 23.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX564169/citrix-secure-access-client-for-ubuntu-security-bulletin-for-cve202324492

Affected Product	**Fortinet**
Severity	**Critical**
Affected Vulnerability	Stack-Based Overflow Vulnerability (CVE-2023-33308)
Description	Fortinet has released a security update addressing a Stack-Based Overflow Vulnerability that exists in FortiOS and FortiProxy. The flaw may allow a remote attacker to execute arbitrary code or command via crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection. Fortinet highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiOS version 7.2.0 through 7.2.3 FortiOS version 7.0.0 through 7.0.10 FortiProxy version 7.2.0 through 7.2.2 FortiProxy version 7.0.0 through 7.0.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-183

Affected Product	**Sap**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerability (CVE-2023-36922)
Description	SAP has released a security update addressing a Command Injection vulnerability within their products. The flaw allows an authenticated attacker to inject an arbitrary operating system command into an unprotected parameter in a common (default) extension. On successful exploitation, the attacker can read or modify the system data as well as shut down the system. Information Disclosure. SAP highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	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	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1829, CVE-2023-3090, CVE-2023-3111, CVE-2023-3212, CVE-2023-3357, CVE-2023-3358, CVE-2023-3389, CVE-2023-1077, CVE-2023-1079, CVE-2023-1249, CVE-2023-1637, CVE-2023-2002, CVE-2023-3141, CVE-2023-3159, CVE-2023-3161, CVE-2023-3268, CVE-2023-35824, CVE-2017-5753, CVE-2018-20784, CVE-2022-3566, CVE-2022-45884, CVE-2022-45885, CVE-2022-45886, CVE-2022-45887, CVE-2022-45919, CVE-2023-0590, CVE-2023-1095, CVE-2023-1118, CVE-2023-1380, CVE-2023-1390, CVE-2023-1513, CVE-2023-1611, CVE-2023-1670, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2124, CVE-2023-2162, CVE-2023-2194, CVE-2023-23454, CVE-2023-23455, CVE-2023-2513, CVE-2023-28328, CVE-2023-28464, CVE-2023-28772, CVE-2023-30772, CVE-2023-31436, CVE-2023-32269, CVE-2020-24588, CVE-2022-2196, CVE-2022-3523, CVE-2022-36280, CVE-2022-38096, CVE-2022-4269, CVE-2022-4744, CVE-2023-0045, CVE-2023-0122, CVE-2023-0179, CVE-2023-0386, CVE-2023-0394, CVE-2023-0461, CVE-2023-0469, CVE-2023-0597, CVE-2023-1075, CVE-2023-1076, CVE-2023-1078, CVE-2023-1382, CVE-2023-1582, CVE-2023-1583, CVE-2023-1652, CVE-2023-1838, CVE-2023-1855, CVE-2023-21102, CVE-2023-21106, CVE-2023-2156, CVE-2023-2176, CVE-2023-2235, CVE-2023-2269, CVE-2023-22998, CVE-2023-23000, CVE-2023-23001, CVE-2023-23004, CVE-2023-23006, CVE-2023-2483, CVE-2023-25012, CVE-2023-26545, CVE-2023-28327, CVE-2023-28410, CVE-2023-28466, CVE-2023-28866, CVE-2023-3006, CVE-2023-30456, CVE-2023-31084, CVE-2023-3220, CVE-2023-32233, CVE-2023-33288, CVE-2023-33951, CVE-2023-33952, CVE-2023-35788, CVE-2023-35823, CVE-2023-35828, CVE-2023-35829)
Description	Suse has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of the most severe vulnerabilities could lead to Denial of Service, Use-after-free Condition, Memory leak, Race condition. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4, 15.5 openSUSE Leap 15.5 openSUSE Leap Micro 5.3 SUSE Linux Enterprise High Performance Computing 12 SP2, 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 12 SP5, 15 SP4, 15 SP5 SUSE Linux Enterprise Server 12 SP2, 12 SP5 SUSE Linux Enterprise Server 12 SP2 BCL 12-SP2 SUSE Linux Enterprise Server 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5 SUSE Real Time Module 15-SP4, 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232803-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232804-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232805-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232809-1 https://www.suse.com/support/update/announcement/2023/suse-su-20232808-1

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2588, CVE-2022-3564)
Description	Redhat has released security updates addressing vulnerabilities within their products. **CVE-2022-2588** - A use-after-free flaw was found in route4_change in the net/sched/cls_route.c filter implementation in the Linux kernel. This flaw allows a local user to crash the system and possibly lead to a local privilege escalation problem. **CVE-2022-3564** - A use-after-free flaw was found in the Linux kernel's L2CAP bluetooth functionality in how a user triggers a race condition by two malicious flows in the L2CAP bluetooth packets. This flaw allows a local or bluetooth connection user to crash the system or potentially escalate privileges. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux Server - AUS 7.7 x86_64 Red Hat Enterprise Linux Server - TUS 7.7 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 7.7 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 7.7 x86_64 Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server - AUS 7.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:4023 https://access.redhat.com/errata/RHSA-2023:4022 https://access.redhat.com/errata/RHSA-2023:4021 https://access.redhat.com/errata/RHSA-2023:4020

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Local Privilege escalation Vulnerability (CVE-2023-24491)
Description	Citrix has released a security update addressing a Local Privilege escalation vulnerability within Citrix Secure Access client for Windows. The flaw is exploited when access to an endpoint with Standard User Account that has the vulnerable client installed Citrix recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Citrix Secure Access client for Windows before 23.5.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX561480/citrix-secure-access-client-for-windows-security-bulletin-for-cve202324491

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35971, CVE-2023-35972, CVE-2023-35973, CVE-2023-35974, CVE-2023-35975, CVE-2023-35976, CVE-2023-35977, CVE-2023-35978, CVE-2023-35979)
Description	HPE has released a security update addressing multiple vulnerabilities within their products. Exploitation of these vulnerabilities leads to Remote Arbitrary Command Execution, Cross-Site Scripting (XSS), Denial of Service (DoS), Directory Traversal, Disclosure of Sensitive Information. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE Aruba Networking - Mobility Conductor (formerly Mobility Master) HPE Aruba Networking - Mobility Controllers HPE Aruba Networking - WLAN Gateways and SD-WAN Gateways managed by Aruba Central ArubaOS 10.4.x.x: 10.4.0.1 and below ArubaOS 8.11.x.x: 8.11.1.0 and below ArubaOS 8.10.x.x: 8.10.0.6 and below ArubaOS 8.6.x.x: 8.6.0.20 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04490en_us

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34472, CVE-2023-34473, CVE-2023-34471, CVE-2023-34337, CVE-2023-34338, CVE-2023-3078, CVE-2023-20575)
Description	Lenovo has released security updates addressing multiple vulnerabilities within their products. Exploitation of these vulnerabilities leads to Sensitive Data Exposure, Privilege Escalation. Lenovo recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HR610X (Hyperscale) - Baseboard Management Controller (BMC) - ThinkSystem HR610X V15_38 HR630X (HyperScale)- Baseboard Management Controller (BMC) - ThinkSystem HR630X/HR650X V11.52 HR650X (Hyperscale)- Baseboard Management Controller (BMC) - ThinkSystem HR630X/HR650X V11.52 Lenovo Universal Device Client (UDC)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-118375 https://support.lenovo.com/us/en/product_security/LEN-121183 https://support.lenovo.com/us/en/product_security/LEN-132938

Affected Product	**SAP**
Severity	**High** ,**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-33989, CVE-2023-33987, CVE-2023-33991, CVE-2023-33990, CVE-2023-35871, CVE-2023-36925, CVE-2023-36921, CVE-2023-35873, CVE-2023-35872, CVE-2023-35870, CVE-2023-33988, CVE-2023-36918, CVE-2023-36920, CVE-2023-36919, CVE-2023-35874, CVE-2023-36917, CVE-2023-31405, CVE-2023-36924, CVE-2023-33992)
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, Directory Traversal, Request smuggling and request concatenation, Denial of service SAP recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	SAP NetWeaver (BI CONT ADD ON), Versions –707, 737, 747, 757 SAP Web Dispatcher, Versions–WEBDISP 7.49, WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.81, WEBDISP 7.85, WEBDISP 7.88, WEBDISP 7.89, WEBDISP 7.90, KERNEL 7.49, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.88, KERNEL 7.89, KERNEL 7.90, KRNL64NUC 7.49, KRNL64UC 7.49, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1 SAP UI5 Variant Management, Versions –SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200 SAP SQL Anywhere, Version-17.0 SAP Web Dispatcher, Versions-WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.85, WEBDISP7.89, WEBDISP 7.91, WEBDISP 7.92, WEBDISP 7.93, KERNEL 7.53, KERNEL 7.54,KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1 SAP Solution Manager (Diagnostic Agent), Versions –7.20 SAP NetWeaver Process Integration (Runtime Workbench), Versions–SAP_XITOOL 7.50 SAP NetWeaver Process Integration (Message Display Tool), Versions–SAP_XIAF 7.50 SAP S/4HANA (Manage Journal Entry Template), Versions–S4CORE 104, 105, 106, 107 SAP Enable Now, Version -WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704 SAP NetWeaver AS ABAP and ABAP Platform, Version -KRNL64NUC7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL7.53, KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.92, KERNEL 7.93 SAP BusinessObjects BI Platform (Enterprise),Version -4.20, 430 SAP NetWeaver AS for Java (Log Viewer), Version -ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50 SAP ERP Defense Forces and Public Security, Version -600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807 SAP Business Warehouseand SAP BW/4HANA, Version -SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300
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	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-30447, CVE-2023-30446, CVE-2023-30443, CVE-2023-30448, CVE-2023-30445, CVE-2023-30449, CVE-2023-30442, CVE-2023-27869, CVE-2023-27867, CVE-2023-27868, CVE-2023-30431, CVE-2023-23487, CVE-2023-27558, CVE-2023-29256, CVE-2023-35012, CVE-2022-39161)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause Arbitrary code execution, Denial of service, Buffer overflow, Privilege Escalation. IBM recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	IBM Db2 10.5.0.11 Server IBM Db2 11.1.4.7 Server IBM Db2 11.5.x Server IBM Db2 10.5.0.11 Client and Server IBM Db2 11.1.4.7 Client and Server IBM Db2 11.5.x Client and Server Jazz Foundation 7, 7.0.1, 7.0.2 IBM Engineering Test Management 7.0.1, 7.0.2 IBM Engineering Workflow Management 7.0.1, 7.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7010557 https://www.ibm.com/support/pages/node/7010561 https://www.ibm.com/support/pages/node/7010029 https://www.ibm.com/support/pages/node/7010565 https://www.ibm.com/support/pages/node/7010567 https://www.ibm.com/support/pages/node/7010571 https://www.ibm.com/support/pages/node/7010573 https://www.ibm.com/support/pages/node/7010747 https://www.ibm.com/support/pages/node/7010659 https://www.ibm.com/support/pages/node/7010655

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	Insufficient session expiration vulnerability (CVE-2023-28001)
Description	Fortinet has released a security update addressing an Insufficient session expiration vulnerability within FortiOS REST API. The flaw allows an attacker to reuse the session of a deleted user, should the attacker manage to obtain the API token. Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiOS version 7.2.0 through 7.2.4 FortiOS 7.0 all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-028

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.