Advisory Alert

Alert Number: AAA20240313 **Date:** March 13, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
FortiGuard	**Critical**	Multiple Vulnerabilities
SAP	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Ubuntu	**High**	Multiple Vulnerabilities
SAP	**High**, Medium	Multiple Vulnerabilities
Intel	**High**, Medium	Multiple Vulnerabilities
Lenovo	**High**, Medium	Multiple Vulnerabilities
F5	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Medium, Low	Multiple Vulnerabilities
FortiGuard	**High**, Medium, Low	Multiple Vulnerabilities
Citrix	**Medium**	Limited Information Disclosure Vulnerability
IBM	**Medium**	Multiple Vulnerabilities
SonicWall	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-48788, CVE-2023-42789, CVE-2023-42790)
Description	FortiGuard has issued security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to unauthorized code or command execution. **CVE-2023-48788** - An improper neutralization of special elements used in an SQL Injection vulnerability in FortiClientEMS may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted requests. **CVE-2023-42789** - A out-of-bounds write in Fortinet allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. **CVE-2023-42790** - A stack-based buffer overflow in Fortinet allows attacker to execute unauthorized code or commands via specially crafted HTTP requests. FortiGuard advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	FortiOS version 7.4.0 through 7.4.1 FortiOS version 7.2.0 through 7.2.5 FortiOS version 7.0.0 through 7.0.12 FortiOS version 6.4.0 through 6.4.14 FortiOS version 6.2.0 through 6.2.15 FortiProxy version 7.4.0 FortiProxy version 7.2.0 through 7.2.6 FortiProxy version 7.0.0 through 7.0.12 FortiProxy version 2.0.0 through 2.0.13 FortiClientEMS v7.2.0 through v7.2.2 FortiClientEMS v7.0.1 through v7.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-328 https://www.fortiguard.com/psirt/FG-IR-24-007

Affected Product	**SAP**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-10744, CVE-2024-22127)
Description	SAP has issued monthly security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by an attacker with high privileges to upload potentially dangerous files which leads to command injection vulnerability. **CVE-2019-10744** - Versions of lodash lower than 4.17.12 are vulnerable to Prototype Pollution. The function defaultsDeep could be tricked into adding or modifying properties of Object.prototype using a constructor payload. **CVE-2024-22127** - SAP NetWeaver allows an attacker with high privileges to upload potentially dangerous files which leads to command injection vulnerability. This would enable the attacker to run commands which can cause high impact on confidentiality, integrity and availability of the application. SAP advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	SAP Business Client v6.5, v7.0, v7.70 SAP Build Apps, Versions prior to 4.9.145 SAP NetWeaver AS Java v7.50
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2024.html

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21392, CVE-2024-26203, CVE-2024-21421, CVE-2024-21390, CVE-2024-21400, CVE-2024-26164, CVE-2024-21419, CVE-2024-26198, CVE-2024-21437, CVE-2024-26201, CVE-2024-26199, CVE-2024-21426, CVE-2024-26190, CVE-2024-21448, CVE-2024-21451, CVE-2024-26161, CVE-2024-26166, CVE-2024-21444, CVE-2024-21450, CVE-2024-21434, CVE-2024-21330, CVE-2024-21334, CVE-2024-26204, CVE-2024-21407, CVE-2024-21408, CVE-2024-21411, CVE-2024-21418, CVE-2024-26165, CVE-2024-21438, CVE-2024-26160, CVE-2024-26170, CVE-2024-26185, CVE-2024-20671, CVE-2024-26169, CVE-2024-21431, CVE-2024-21436, CVE-2024-21427, CVE-2024-26177, CVE-2024-26176, CVE-2024-26174, CVE-2024-26182, CVE-2024-26181, CVE-2024-26178, CVE-2024-26173, CVE-2024-21443, CVE-2024-21446, CVE-2024-21440, CVE-2024-26162, CVE-2024-26159, CVE-2024-21435, CVE-2024-21433, CVE-2024-26197, CVE-2024-21439, CVE-2024-21432, CVE-2024-21429, CVE-2024-21442, CVE-2024-21445, CVE-2024-21430)
Description	Microsoft has released critical security updates for March 2024. This release includes fixes for several vulnerabilities across various Microsoft products. It is highly recommended that you apply these security patches immediately to protect your systems from potential threats.
Affected Products	.NET 7.0 build 7.0.17 .NET 8.0 build 8.0.3 Azure Automation OMS Agent for Linux GA 1.19.0 Azure Automation Update Management OMS Agent for Linux GA v1.19.0 Azure Data Studio v1.48.0 Azure Kubernetes Service Confidential Containers v0.3.3 Azure SDK v1.29.5 Azure Security Center OMS Agent for Linux GA 1.19.0 Azure Sentinel OMS Agent for Linux GA v1.19.0 Container Monitoring Solution ID: sha256:855bfeb0 Intune Company Portal for Android 2402 Log Analytics Agent OMS Agent for Linux GA v1.19.0 Microsoft 365 Apps for Enterprise for 64-bit Systems Microsoft Authenticator v6.2401.0617 Microsoft Dynamics 365 (on-premises) version 9.1 build 9.1.26 Microsoft Exchange Server 2016 Cumulative Update 23 v15.01.2507.037 Microsoft Exchange Server 2019 Cumulative Update 13 v15.02.1258.032 Microsoft Exchange Server 2019 Cumulative Update 14 v15.02.1544.009 Microsoft Outlook for Android v4.2404.0 Microsoft SharePoint Enterprise Server 2016 v16.0.5439.1000 Microsoft SharePoint Server 2019 v16.0.10408.20000 Microsoft SharePoint Server Subscription Edition v16.0.17328.20136 Microsoft Teams for Android v1.0.0.2024022302 Microsoft Visual Studio 2022 version 17.4 build 17.4.17 Microsoft Visual Studio 2022 version 17.6 build 17.6.13 Microsoft Visual Studio 2022 version 17.8 build 17.8.8 Microsoft Visual Studio 2022 version 17.9 build17.9.3 Open Management Infrastructure OMI v1.8.1-0 Operations Management Suite Agent for Linux (OMS) v1.8.1-0 Skype for Consumer v8.113 Software for Open Networking in the Cloud (SONiC) 201811 v20181130.106 Software for Open Networking in the Cloud (SONiC) 201911 v20191130.89 Software for Open Networking in the Cloud (SONiC) 202012 v20201231.96 Software for Open Networking in the Cloud (SONiC) 202205 v20220531.26 SQL Server backend for Django v1.4.1 System Center Operations Manager (SCOM) 2019 v10.19.1253.0 System Center Operations Manager (SCOM) 2022 v10.22.1070.0 Visual Studio Code v1.87.2 Windows 10 for 32-bit Systems v10.0.10240.20526 Windows 10 for x64-based Systems v10.0.10240.20526 Windows 10 Version 1607 for 32-bit Systems v10.0.14393.6796 Windows 10 Version 1607 for x64-based Systems v10.0.14393.6796 Windows 10 Version 1809 for 32-bit Systems v10.0.17763.5576 Windows 10 Version 1809 for ARM64-based Systems v10.0.17763.5576 Windows 10 Version 1809 for x64-based Systems v10.0.17763.5576 Windows 10 Version 21H2 for 32-bit Systems v10.0.19044.4170 Windows 10 Version 21H2 for ARM64-based Systems v10.0.19044.4170 Windows 10 Version 21H2 for x64-based Systems v10.0.19044.4170 Windows 10 Version 22H2 for 32-bit Systems v10.0.19045.4170 Windows 10 Version 22H2 for ARM64-based Systems v10.0.19045.4170 Windows 10 Version 22H2 for x64-based Systems v10.0.19045.4170 Windows 11 version 21H2 for ARM64-based Systems v10.0.22000.2836 Windows 11 version 21H2 for x64-based Systems v10.0.22000.2836 Windows 11 Version 22H2 for ARM64-based Systems v10.0.22621.3296 Windows 11 Version 22H2 for x64-based Systems v10.0.22621.3296 Windows 11 Version 23H2 for ARM64-based Systems v10.0.22631.3296 Windows 11 Version 23H2 for x64-based Systems v10.0.22631.3296 Windows Defender Antimalware Platform v4.18.24010.12 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) v6.0.6003.22567 Windows Server 2008 for 32-bit Systems Service Pack 2 v6.0.6003.22567 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) v6.0.6003.22567 Windows Server 2008 for x64-based Systems Service Pack 2 v6.0.6003.22567 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) v6.1.7601.27017 Windows Server 2008 R2 for x64-based Systems Service Pack 1 v6.1.7601.27017 Windows Server 2012 (Server Core installation) v6.2.9200.24768 Windows Server 2012 R2 (Server Core installation) v6.3.9600.21871 Windows Server 2012 R2 v6.3.9600.21871 Windows Server 2012 v6.2.9200.24768 Windows Server 2016 (Server Core installation) v10.0.14393.6796 Windows Server 2016 v10.0.14393.6796 Windows Server 2019 (Server Core installation) v10.0.17763.5576 Windows Server 2019 v10.0.17763.5576 Windows Server 2022 (Server Core installation) v10.0.20348.2333 Windows Server 2022 (Server Core installation) v10.0.20348.2340 Windows Server 2022 v10.0.20348.2333 Windows Server 2022 v10.0.20348.2340 Windows Server 2022, 23H2 Edition (Server Core installation) v10.0.25398.763
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Mar

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35191, CVE-2023-22655, CVE-2023-39368, CVE-2023-38575, CVE-2023-28746, CVE-2023-32282.)
Description	HPE has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to Arbitrary Code Execution, Remote Denial of Service, Local Privilege Escalation and Information Disclosure. HPE recommends to apply the necessary patch updates at your earliest to protect your systems from potential threats.
Affected Products	HPE Synergy 480 Gen10 Plus Compute Module Prior to v04.04.04.603.0, Prior to v2.00_02-22-2024 HPE ProLiant XL220n Gen10 Plus Server Prior to v04.04.04.603.0, Prior to v2.00_02-22-2024 HPE ProLiant XL290n Gen10 Plus Server Prior to v04.04.04.603.0, Prior to v2.00_02-22-2024 HPE ProLiant DL20 Gen11 Prior to v1.44_01-18-2024 HPE ProLiant DL20 Gen10 Plus server - Prior to v2.00_02-01-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v2.00_02-01-2024 HPE ProLiant MicroServer Gen11 - Prior to v1.44_01-18-2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.00_02-01-2024 HPE ProLiant ML30 Gen11 Prior to v1.44_01-18-2024 HPE Apollo 2000 Gen10 Plus System Prior to v04.04.04.603.0, Prior to v2.00_02-22-2024 HPE Apollo 4200 Gen10 Plus System Prior to v04.04.04.603.0, Prior to v2.00_02-22-2024 HPE Edgeline e920t Server Blade Prior to v2.00_02-22-2024, Prior to v04.04.04.603.0 HPE Edgeline e920 Server Blade Prior to v2.00_02-22-2024, Prior to v04.04.04.603.0 HPE Edgeline e920d Server Blade Prior to v2.00_02-22-2024, Prior to v04.04.04.603.0 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.00_02-22-2024, Prior to v04.04.04.603.0 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.00_03-06-2024, Prior to v04.04.04.603.0 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.00_03-06-2024, Prior to v04.04.04.603.0 HPE ProLiant DX360 Gen10 Plus server - Prior to v2.00_03-06-2024, Prior to v04.04.04.603.0 HPE ProLiant DX380 Gen10 Plus server - Prior to v2.00_03-06-2024, Prior to v04.04.04.603.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04616en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04623en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04614en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04615en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04612en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04613en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04608en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04609en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04606en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04607en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04602en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04605en_us

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6817, CVE-2023-6932, CVE-2023-7192, CVE-2024-0193, CVE-2024-0646)
Description	Ubuntu has released security updates addressing multiple vulnerabilities in Ubuntu Linux Kernel. If exploited, these vulnerabilities could lead to Arbitrary Code Execution or Denial of Service. Ubuntu recommends to apply the necessary patch updates at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0101-1

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39439, CVE-2023-44487, CVE-2023-50164, CVE-2024-27902, CVE-2024-25644, CVE-2024-25645, CVE-2024-28163, CVE-2024-22133, CVE-2024-27900)
Description	SAP has issued monthly security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities may allow attackers to cause Denial of service, Information Disclosure, Improper Access Control, Cross-Site Scripting and Path Traversal exploits. SAP advises to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	SAP Commerce versions - HY_COM 2105, HY_COM 2205, COM_CLOUD 2211 SAP HANA Database v2.0 SAP HANA Extended Application Services Advanced (XS Advanced) v1.0 SAP BusinessObjects Business Intelligence Platform (Central Management Console) v4.3 SAP NetWeaver AS ABAP applications based on SAPGUI for HTML (WebGUI) versions 7.89, 7.93 SAP NetWeaver (WSRM) v7.50 SAP NetWeaver (Enterprise Portal) v7.50 SAP NetWeaver Process Integration (Support Web Pages) v7.50 SAP Fiori Front End Server v605 SAP ABAP Platform versions - 758, 795
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2024.html

Affected Product	**Intel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28746, CVE-2023-35191, CVE-2023-28389, CVE-2023-32633, CVE-2023-27502, CVE-2023-32282, CVE-2023-22655, CVE-2023-39368, CVE-2023-38575, CVE-2023-32666, CVE-2023-43490)
Description	Intel has released security updates addressing multiple vulnerabilities that exist in Intel hardware and firmware components. These vulnerabilities could be exploited by malicious users to cause denial of service, escalation of privilege, information disclosure. Intel recommends to apply the necessary patch updates at your earliest to protect your systems from potential threats.
Affected Products	Multiple Intel Hardware and Firmware components
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00898.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00923.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00929.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00960.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00972.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00982.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00982.html https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01045.html

Affected Product	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-5952, CVE-2022-30426, CVE-2023-22655, CVE-2023-28149, CVE-2023-28746, CVE-2023-32282, CVE-2023-32666, CVE-2023-35191, CVE-2023-27502, CVE-2023-28389, CVE-2023-38575, CVE-2023-39281, CVE-2023-39283, CVE-2023-39284, CVE-2023-39368, CVE-2023-5912, CVE-2023-32633)
Description	Lenovo has released security updates addressing multiple vulnerabilities in their products. If exploited, these vulnerabilities could lead to Arbitrary Code Execution, Denial of Service, Privilege Escalation and Information Disclosure. Lenovo recommends to apply the necessary patch updates at your earliest to protect your systems from potential threats.
Affected Products	Multiple Lenovo Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-155477 https://support.lenovo.com/us/en/product_security/LEN-142128

Affected Product	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-22218, CVE-2022-21216)
Description	F5 has released security updates addressing multiple vulnerabilities in F5OS. If exploited, these vulnerabilities could lead to disclosure of information from process memory and escalation of privilege through adjacent network access. F5 recommends to apply the necessary patch updates at your earliest to protect your systems from potential threats.
Affected Products	F5OS-A v1.5.0 - v1.5.1, v1.4.0, v1.3.0 - v1.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000133432 https://my.f5.com/manage/s/article/K000138219

Affected Product	**Dell**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-47534, CVE-2023-41842, CVE-2024-23112, CVE-2023-46717, CVE-2024-21761, CVE-2023-36554)
Description	Dell has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. It is recommended by Dell to apply necessary security fixes at your earliest to protect your systems from potential threats.
.Affected Products	Multiple Dell Hardware and Firmware components
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222812/dsa-2024-004-security-update-for-dell-poweredge-server-bios-for-an-improper-smm-communication-buffer-verification-vulnerability https://www.dell.com/support/kbdoc/en-us/000222756/dsa-2024-003-security-update-for-dell-poweredge-server-bios-for-a-time-of-check-time-of-use-toctou-vulnerability https://www.dell.com/support/kbdoc/en-us/000222891/dsa-2024-005-security-update-for-dell-poweredge-server-for-intel-march-2024-security-advisories-2024-1-ipu https://www.dell.com/support/kbdoc/en-us/000217983/dsa-2023-364 https://www.dell.com/support/kbdoc/en-us/000223032/dsa-2024-130-security-update-for-dell-emc-metro-node-for-multiple-third-party-component-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000218769/dsa-2023-395 https://www.dell.com/support/kbdoc/en-us/000223008/dsa-2024-128-security-update-for-dell-poweredge-t30-t40-mini-tower-server-for-intel-march-2024-security-advisories-2024-1-ipu https://www.dell.com/support/kbdoc/en-us/000222979/dsa-2024-006-security-update-for-dell-poweredge-server-bios-for-an-improper-smm-communication-buffer-verification-vulnerability https://www.dell.com/support/kbdoc/en-us/000222898/dsa-2024-034-security-update-for-dell-poweredge-server-bios-for-an-improper-parameter-initialization-vulnerability https://www.dell.com/support/kbdoc/en-us/000220797/dsa-2024-036-security-update-for-dell-platform-bios-multiple-third-party-component-vulnerabilities

Affected Product	**FortiGuard**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-47534, CVE-2023-41842, CVE-2024-23112, CVE-2023-46717, CVE-2024-21761, CVE-2023-36554)
Description	FortiGuard has issued security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities may allow remote, unauthenticated and privileged attackers to execute arbitrary commands, URL manipulation, gain read-write access and download other organizations reports. It is recommended by FortiGuard to apply necessary security fixes at your earliest to protect your systems from potential threats.
.Affected Products	FortiClientEMS versions 7.2.0 through 7.2.2 FortiClientEMS versions 7.0.0 through 7.0.10 FortiClientEMS 6.4 all versions FortiClientEMS 6.2 all versions FortiClientEMS 6.0 all versions FortiManager versions 7.4.0 through 7.4.1 FortiManager versions 7.2.0 through 7.2.3 FortiManager 7.0 all versions FortiManager 6.4 all versions FortiManager 6.2 all versions FortiAnalyzer versions 7.4.0 through 7.4.1 FortiAnalyzer versions 7.2.0 through 7.2.3 FortiAnalyzer 7.0 all versions FortiAnalyzer 6.4 all versions FortiAnalyzer 6.2 all versions FortiAnalyzer-BigData versions 7.2.0 through 7.2.5 FortiAnalyzer-BigData versions 7.0.1 through 7.0.6 FortiAnalyzer-BigData versions 6.4.5 through 6.4.7 FortiAnalyzer-BigData versions 6.2.5 FortiPortal version 7.2.0 FortiPortal versions 7.0.0 through 7.0.6 FortiPortal versions 6.0.0 through 6.0.14 FortiPortal 5.3 all versions FortiOS versions 7.4.0 through 7.4.1 FortiOS versions 7.2.0 through 7.2.6 FortiOS versions 7.0.1 through 7.0.13 FortiOS versions 6.4.7 through 6.4.14 FortiProxy versions 7.4.0 through 7.4.2 FortiProxy versions 7.2.0 through 7.2.8 FortiProxy versions 7.0.0 through 7.0.14
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-390 https://www.fortiguard.com/psirt/FG-IR-23-304 https://www.fortiguard.com/psirt/FG-IR-24-013 https://www.fortiguard.com/psirt/FG-IR-23-424 https://www.fortiguard.com/psirt/FG-IR-24-016 https://www.fortiguard.com/psirt/FG-IR-23-103

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Limited Information Disclosure Vulnerability (CVE-2024-2049)
Description	Citrix has issued security updates addressing a Limited Information Disclosure Vulnerability that exist Citrix SDWAN. Server-Side Request Forgery (SSRF) in Citrix SD-WAN Standard/Premium Editions on or after 11.4.0 and before 11.4.4.46 allows an attacker to disclose limited information from the appliance via Access to management IP. It is recommended by Citrix to apply necessary security fixes at your earliest to protect your systems from potential threats.
.Affected Products	SD-WAN Standard/Premium Editions on or after 11.4.0 and before 11.4.4.46
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX617071/citrix-sdwan-security-bulletin-for-cve20242049

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-46158, CVE-2023-22081, CVE-2023-22067, CVE-2023-5676)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to denial of service and improper resource expiration handling. It is recommended by IBM to apply necessary security fixes at your earliest to protect your systems from potential threats.
.Affected Products	IBM TXSeries for Multiplatforms v8.1 IBM TXSeries for Multiplatforms v8.2 IBM TXSeries for Multiplatforms v9.1 HMC V10.1.1010.0 HMC V10.2.1030.0 HMC V10.3.1050.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7109965 https://www.ibm.com/support/pages/node/7138007

Affected Product	**SonicWall**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22398, CVE-2024-22397, CVE-2024-22396)
Description	SonicWall has issued security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to directory traversal attacks, Cross-Site Scripting and Integer-based buffer overflow. It is recommended by SonicWall to apply necessary security fixes at your earliest to protect your systems from potential threats.
Affected Products	SonicWall Email Security Appliance 10.0.26.7807 and earlier versions. SonicOS 7.0.1-5145 and older versions, 7.1.1-7047 and older versions Gen7 - TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700, NSv 270, NSv 470, NSv 870 SonicOS 6.5.4.4-44v-21-2340 and older versions Gen6 SonicOSv - NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) on VMWare, NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) on Hyper-V, NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) on KVM, NSv (200, 400, 800, 1600) on AWS NSv (200, 400, 800, 1600) on AWS-PAYG, NSv (200, 400, 800, 1600) on Azure SonicOS 6.5.4.13-105n and older versions Gen6 Firewalls -SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0004 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0005 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0006

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.