Advisory Alert

Alert Number: AAA20240410 **Date:** April 10, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
FortiGuard	**Critical**	Code Injection vulnerability
SAP	**High**, Medium	Multiple Vulnerabilities
FortiGuard	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities
Lenovo	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
Dell	Medium	Multiple Vulnerabilities

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-0001, CVE-2023-24932, CVE-2024-20665, CVE-2024-20669, CVE-2024-20670, CVE-2024-20678, CVE-2024-20685, CVE-2024-20688, CVE-2024-20689, CVE-2024-20693, CVE-2024-21322, CVE-2024-21323, CVE-2024-21324, CVE-2024-21330, CVE-2024-21409, CVE-2024-21424, CVE-2024-21427, CVE-2024-21447, CVE-2024-23593, CVE-2024-23594, CVE-2024-26158, CVE-2024-26168, CVE-2024-26171, CVE-2024-26172, CVE-2024-26175, CVE-2024-26179, CVE-2024-26180, CVE-2024-26183, CVE-2024-26189, CVE-2024-26193, CVE-2024-26194, CVE-2024-26195, CVE-2024-26200, CVE-2024-26202, CVE-2024-26205, CVE-2024-26207, CVE-2024-26208, CVE-2024-26209, CVE-2024-26210, CVE-2024-26211, CVE-2024-26212, CVE-2024-26213, CVE-2024-26214, CVE-2024-26215, CVE-2024-26216, CVE-2024-26217, CVE-2024-26218, CVE-2024-26219, CVE-2024-26220, CVE-2024-26221, CVE-2024-26222, CVE-2024-26223, CVE-2024-26224, CVE-2024-26226, CVE-2024-26227, CVE-2024-26228, CVE-2024-26229, CVE-2024-26230, CVE-2024-26231, CVE-2024-26232, CVE-2024-26233, CVE-2024-26234, CVE-2024-26235, CVE-2024-26236, CVE-2024-26237, CVE-2024-26239, CVE-2024-26240, CVE-2024-26241, CVE-2024-26242, CVE-2024-26243, CVE-2024-26244, CVE-2024-26245, CVE-2024-26248, CVE-2024-26250, CVE-2024-26251, CVE-2024-26252, CVE-2024-26253, CVE-2024-26254, CVE-2024-26255, CVE-2024-26256, CVE-2024-26257, CVE-2024-28896, CVE-2024-28897, CVE-2024-28898, CVE-2024-28900, CVE-2024-28901, CVE-2024-28902, CVE-2024-28903, CVE-2024-28904, CVE-2024-28905, CVE-2024-28906, CVE-2024-28907, CVE-2024-28908, CVE-2024-28909, CVE-2024-28910, CVE-2024-28911, CVE-2024-28912, CVE-2024-28913, CVE-2024-28914, CVE-2024-28915, CVE-2024-28917, CVE-2024-28919, CVE-2024-28920, CVE-2024-28921, CVE-2024-28922, CVE-2024-28923, CVE-2024-28924, CVE-2024-28925, CVE-2024-28926, CVE-2024-28927, CVE-2024-28929, CVE-2024-28930, CVE-2024-28931, CVE-2024-28932, CVE-2024-28933, CVE-2024-28934, CVE-2024-28935, CVE-2024-28936, CVE-2024-28937, CVE-2024-28938, CVE-2024-28939, CVE-2024-28940, CVE-2024-28941, CVE-2024-28942, CVE-2024-28943, CVE-2024-28944, CVE-2024-28945, CVE-2024-29043, CVE-2024-29044, CVE-2024-29045, CVE-2024-29046, CVE-2024-29047, CVE-2024-29048, CVE-2024-29050, CVE-2024-29052, CVE-2024-29053, CVE-2024-29054, CVE-2024-29055, CVE-2024-29056, CVE-2024-29061, CVE-2024-29062, CVE-2024-29063, CVE-2024-29064, CVE-2024-29066, CVE-2024-29982, CVE-2024-29983)
Description	Microsoft has released security updates for April 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 systems from potential threats.
Affected Products	Windows Server 2022, 23H2 Edition (Server Core installation) Build Number 10.0.25398.830 Windows Server 2022 (Server Core installation) Build Number 10.0.20348.2402 Windows Server 2022 Build Number 10.0.20348.2402 Windows Server 2019 (Server Core installation) Build Number 10.0.17763.5696 Windows Server 2019 Build Number 10.0.17763.5696 Windows Server 2016 (Server Core installation) Build Number 10.0.14393.6897 Windows Server 2016 Build Number 10.0.14393.6897 Windows Server 2012 R2 (Server Core installation) Build Number 6.3.9600.21924 Windows Server 2012 R2 Build Number 6.3.9600.21924 Windows Server 2012 (Server Core installation) Build Number 6.2.9200.24821 Windows Server 2012 Build Number 6.2.9200.24821 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) Build Number 6.0.6003.22618 Windows Server 2008 for x64-based Systems Service Pack 2 Build Number 6.0.6003.22618 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) Build Number 6.0.6003.22618 Windows Server 2008 for 32-bit Systems Service Pack 2 Build Number 6.0.6003.22618 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Build Number 6.1.7601.27067 Windows Server 2008 R2 for x64-based Systems Service Pack 1 Build Number 6.1.7601.27067 Windows 11 version 21H2 for x64-based Systems Build Number 10.0.22000.2899 Windows 11 version 21H2 for ARM64-based Systems Build Number 10.0.22000.2899 Windows 11 Version 23H2 for x64-based Systems Build Number 10.0.22631.3447 Windows 11 Version 23H2 for ARM64-based Systems Build Number 10.0.22631.3447 Windows 11 Version 22H2 for x64-based Systems Build Number 10.0.22621.3435 Windows 11 Version 22H2 for ARM64-based Systems Build Number 10.0.22621.3435 Windows 10 for x64-based Systems Build Number 10.0.10240.20596 Windows 10 for 32-bit Systems Build Number 10.0.10240.20596 Windows 10 Version 22H2 for x64-based Systems Build Number 10.0.19045.4291 Windows 10 Version 22H2 for ARM64-based Systems Build Number 10.0.19045.4291 Windows 10 Version 22H2 for 32-bit Systems Build Number 10.0.19045.4291 Windows 10 Version 21H2 for x64-based Systems Build Number 10.0.19044.4291 Windows 10 Version 21H2 for ARM64-based Systems Build Number 10.0.19044.4291 Windows 10 Version 21H2 for 32-bit Systems Build Number 10.0.19044.4291 Windows 10 Version 1809 for x64-based Systems Build Number 10.0.17763.5696 Windows 10 Version 1809 for ARM64-based Systems Build Number 10.0.17763.5696 Windows 10 Version 1809 for 32-bit Systems Build Number 10.0.17763.5696 Windows 10 Version 1607 for x64-based Systems Build Number 10.0.14393.6897 Windows 10 Version 1607 for 32-bit Systems Build Number 10.0.14393.6897 Outlook for Windows Build Number 1.2023.0322.0100 Microsoft Visual Studio 2022 version 17.9 Build Number 17.9.6 Microsoft Visual Studio 2022 version 17.8 Build Number 17.8.9 Microsoft Visual Studio 2022 version 17.6 Build Number 17.6.14 Microsoft Visual Studio 2022 version 17.4 Build Number 17.4.18

	Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) Build Number 16.11.35 Microsoft SharePoint Server Subscription Edition Build Number 16.0.17328.20246 Microsoft SharePoint Server 2019 Build Number 16.0.10409.20027 Microsoft SharePoint Server 2016 Build Number 16.0.5443.1000 Microsoft SQL Server 2022 for x64-based Systems (GDR) Build Number 16.0.1115.1 Microsoft SQL Server 2022 for x64-based Systems (CU 12) Build Number 16.0.4120.1 Microsoft SQL Server 2019 for x64-based Systems (GDR) Build Number 15.0.2110.4 Microsoft SQL Server 2019 for x64-based Systems (CU 25) Build Number 15.0.4360.2 Microsoft OLE DB Driver 19 for SQL Server Build Number 19.3.0003.0 Microsoft OLE DB Driver 18 for SQL Server Build Number 18.7.0002.0 Microsoft ODBC Driver 18 for SQL Server on Windows Build Number 18.3.3.1 Microsoft ODBC Driver 18 for SQL Server on MacOS Build Number 18.3.3.1 Microsoft ODBC Driver 18 for SQL Server on Linux Build Number 18.3.3.1 Microsoft ODBC Driver 17 for SQL Server on Windows Build Number 17.10.6.1 Microsoft ODBC Driver 17 for SQL Server on MacOS Build Number 17.10.6.1 Microsoft ODBC Driver 17 for SQL Server on Linux Build Number 17.10.6.1 Microsoft Defender for IoT Build Number 24.1.3 Microsoft 365 Apps for Enterprise for 64-bit Systems Build Number https://aka.ms/OfficeSecurityReleases Microsoft 365 Apps for Enterprise for 32-bit Systems Build Number https://aka.ms/OfficeSecurityReleases Microsoft .NET Framework 4.8 Build Number 4.8.4718.0 Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 Build Number 4.7.4092.0 Microsoft .NET Framework 4.6.2 Build Number 4.7.4092.0 Microsoft .NET Framework 3.5 AND 4.8.1 Build Number 4.8.9236.0 Microsoft .NET Framework 3.5 AND 4.8.1 Build Number 4.8.9206.0 Microsoft .NET Framework 3.5 AND 4.8 Build Number 4.8.4718.0 Microsoft .NET Framework 3.5 AND 4.7.2 Build Number 10.0.14393.6897 Microsoft .NET Framework 3.5 AND 4.7.2 Build Number 4.7.4092.0 Azure Private 5G Core Build Number 2403.0-2 Azure Monitor Agent Build Number 1.24.0 Azure Migrate Build Number 6.1.294.1003 Azure Kubernetes Service Confidential Containers Build Number 0.3.4 Azure Identity Library for .NET Build Number 1.11.0 Azure CycleCloud 8.6.0 Build Number 8.6.1 Azure Compute Gallery Build Number Azure Arc Cluster microsoft.videoindexer Extension Build Number 1.1.2 Azure Arc Cluster microsoft.openservicemesh Extension Build Number 1.2.6 Azure Arc Cluster microsoft.networkfabricserviceextension Extension Build Number 5.1.3 Azure Arc Cluster microsoft.iotoperations.mq Extension Build Number 0.3.0-preview Azure Arc Cluster microsoft.azurekeyvaultsecretsprovider Extension Build Number 1.5.2 Azure Arc Cluster microsoft.azure.hybridnetwork Extension Build Number 1.0.2620-162 Azure Arc Cluster microsoft.azstackhci.operator Extension Build Number 5.0.5 Azure AI Search Build Number .NET 8.0 Build Number 8.0.4 .NET 7.0 Build Number 7.0.18 .NET 6.0 Build Number 6.0.29
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Apr

Affected Product	**FortiGuard**
Severity	**Critical**
Affected Vulnerability	Code Injection vulnerability (CVE-2023-45590)
Description	FortiGuard has released security updates addressing a Code Injection vulnerability that exists in FortiClientLinux. **CVE-2023-45590** - An Improper Control of Generation of Code ('Code Injection') vulnerability in FortiClientLinux may allow an unauthenticated attacker to execute arbitrary code via misleading a FortiClientLinux user into visiting a malicious website. FortiGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiClientLinux 7.2 Versions 7.2.0 FortiClientLinux 7.0 Versions 7.0.6 through 7.0.10 FortiClientLinux 7.0 Versions 7.0.3 through 7.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-087

Affected Product	**SAP**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27899, CVE-2024-25646, CVE-2024-27901, CVE-2024-30218, CVE-2024-28167, CVE-2022-29613, CVE-2023-40306, CVE-2024-27898, CVE-2024-30214, CVE-2024-30215, CVE-2024-30216, CVE-2024-30217)
Description	SAP has issued monthly security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Information Disclosure, Directory Traversal, Stack overflow, URL Redirection, Server-Side Request Forgery, Cross-Site Scripting. SAP recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP NetWeaver AS Java User Management Engine Versions: SERVERCORE 7.50, J2EE-APPS 7.50, UMEADMIN 7.50 SAP BusinessObjects Web Intelligence Versions: 4.2, 4.3 SAP Asset Accounting Versions: SAP_APPL 600, SAP_FIN617, SAP_FIN 618, SAP_FIN700 SAP Edge Integration Cell Versions: Older than 8.13.5 SAP NetWeaver AS ABAP and ABAP Platform Versions: KRNL64NUC 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL 7.53, KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.93 SAP Group Reporting Data Collection (Enter Package Data) Versions: S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108, SAP_GRDC_CLOUD 1.0.0 SAP Employee Self Service (Fiori My Leave Request) Version: 605 SAP S/4HANA (Manage Catalog Items and Cross-Catalog search) Versions: S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106 SAP NetWeaver Version: 7.50 SAP Business Connector Version: 4.8 SAP S/4 HANA (Cash Management) Versions: S4CORE 103, S4CORE 104, S4CORE 105, S4CORE 106, S4CORE 107, S4CORE 108
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/april-2024.html

Affected Product	**FortiGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-41677, CVE-2023-45588, CVE-2023-47540, CVE-2023-47541, CVE-2023-47542, CVE-2023-48784, CVE-2024-21755, CVE-2024-21756, CVE-2024-23662, CVE-2024-23671, CVE-2024-31487, CVE-2024-31492)
Description	FortiGuard has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to execute arbitrary code or commands, sensitive information disclosure. FortiGuard recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	FortiClientMac versions 7.0.6 through 7.0.10 FortiClientMac versions 7.2.0 through 7.2.3 FortiManager versions 7.0.0 through 7.0.10 FortiManager versions 7.2.0 through 7.2.4 FortiManager versions 7.4.0 through 7.4.1 FortiOS 6.0 all versions FortiOS versions 6.2.0 through 6.2.15 FortiOS 6.4 all versions FortiOS 7.0 all versions FortiOS versions 7.2.0 through 7.2.7 FortiOS versions 7.4.0 through 7.4.1 FortiProxy 1.0 all versions FortiProxy 1.1 all versions FortiProxy 1.2 all versions FortiProxy 2.0 all versions FortiProxy versions 7.0.0 through 7.0.13 FortiProxy versions 7.2.0 through 7.2.7 FortiProxy versions 7.4.0 through 7.4.1 FortiSandbox 2.0 all versions FortiSandbox 2.1 all versions FortiSandbox 2.2 all versions FortiSandbox 2.3 all versions FortiSandbox 2.4 all versions FortiSandbox 2.5 all versions FortiSandbox 3.0 all versions FortiSandbox 3.1 all versions FortiSandbox 3.2 all versions FortiSandbox 4.0 all versions FortiSandbox versions 4.2.0 through 4.2.6 FortiSandbox versions 4.4.0 through 4.4.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.fortiguard.com/psirt/FG-IR-23-224 • https://www.fortiguard.com/psirt/FG-IR-23-345 • https://www.fortiguard.com/psirt/FG-IR-23-411 • https://www.fortiguard.com/psirt/FG-IR-23-413 • https://www.fortiguard.com/psirt/FG-IR-23-416 • https://www.fortiguard.com/psirt/FG-IR-23-419 • https://www.fortiguard.com/psirt/FG-IR-23-454 • https://www.fortiguard.com/psirt/FG-IR-23-489 • https://www.fortiguard.com/psirt/FG-IR-23-493 • https://www.fortiguard.com/psirt/FG-IR-24-060

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38729, CVE-2023-46234, CVE-2023-45857, CVE-2023-26159, CVE-2023-48795, CVE-2023-37920, CVE-2023-43804, CVE-2023-32681, CVE-2024-26130, CVE-2023-49083)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to sensitive information disclosure, cross-site scripting attacks, Web cache poisoning, denial of service conditions. IBM recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar App SDK 2.2.0 IBM QRadar Deployment Intelligence App1.0.0 - 3.0.12 IBM Db2 10.5.0.x Server IBM Db2 11.1.4.x Server IBM Db2 11.5.x Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145721 • https://www.ibm.com/support/pages/node/7147813 • https://www.ibm.com/support/pages/node/7147812

Affected Product	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28863, CVE-2024-23593, CVE-2024-23594, CVE-2023-4855, CVE-2023-4856, CVE-2023-4857, CVE-2024-2659)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Code Execution, Privilege Escalation, Denial of Service, and Information Disclosure. Lenovo recommends to apply security fixes at your earliest to protect 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-121190 • https://support.lenovo.com/us/en/product_security/LEN-132277 • https://support.lenovo.com/us/en/product_security/LEN-140420

Affected Product	**Ubuntu**
Severity	**High**, **Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1194, CVE-2023-32254, CVE-2023-32258, CVE-2023-38427, CVE-2023-38430, CVE-2023-38431, CVE-2023-3867, CVE-2023-46838, CVE-2023-50431, CVE-2023-52340, CVE-2023-52429, CVE-2023-52434, CVE-2023-52435, CVE-2023-52436, CVE-2023-52438, CVE-2023-52439, CVE-2023-52441, CVE-2023-52442, CVE-2023-52443, CVE-2023-52444, CVE-2023-52445, CVE-2023-52448, CVE-2023-52449, CVE-2023-52451, CVE-2023-52454, CVE-2023-52456, CVE-2023-52457, CVE-2023-52458, CVE-2023-52462, CVE-2023-52463, CVE-2023-52464, CVE-2023-52467, CVE-2023-52469, CVE-2023-52470, CVE-2023-52480, CVE-2023-52609, CVE-2023-52610, CVE-2023-52612, CVE-2023-6610, CVE-2024-0607, CVE-2024-22705, CVE-2024-23850, CVE-2024-23851, CVE-2024-24860, CVE-2024-26586, CVE-2024-26589, CVE-2024-26591, CVE-2024-26597, CVE-2024-26598, CVE-2024-26631, CVE-2024-26633)
Description	Ubuntu has released security updates addressing multiple vulnerabilities in Ubuntu Linux Kernel. If exploited, these vulnerabilities could lead to sensitive Information exposure, arbitrary code execution and Denial of Service conditions. Ubuntu recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 18.04 ESM Ubuntu 20.04 LTS Ubuntu 22.04 LTS Ubuntu 23.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6726-1 • https://ubuntu.com/security/notices/USN-6725-1 • https://ubuntu.com/security/notices/USN-6724-1

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0158, CVE-2023-20593, CVE-2024-22448)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to cause, Out-of-Bounds Write, Cross-Process Information Leak, Denial of Service and escalation of privileges. **CVE-2024-0158-** Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with admin privileges may potentially exploit this vulnerability to modify a UEFI variable, leading to denial of service and escalation of privileges. **CVE-2023-20593 -** Dell Client Platform AMD BIOS contains a Cross-Process Information Leak Vulnerability that could be exploited by malicious users to compromise the affected system. **CVE-2024-22448-** Dell BIOS contains an Out-of-Bounds Write vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to denial of service Dell recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Inspiron 15 3530 BIOS Versions prior to 1.10.0 Latitude 9440 2-in-1 BIOS Versions prior to 1.10.0 Vostro 14 3430 BIOS Versions prior to 1.10.0 Vostro 15 3530 BIOS Versions prior to 1.10.0 XPS 17 9730 BIOS Versions prior to 1.11.0 Vostro 15 3535 BIOS Versions prior to 1.12.0 Latitude 5340 BIOS Versions prior to 1.12.0 Latitude 5540 BIOS Versions prior to 1.12.0 Precision 3580 BIOS Versions prior to 1.12.0 Precision 3581 BIOS Versions prior to 1.12.0 Alienware x14 R2 BIOS Versions prior to 1.13.0 Alienware x16 R1 BIOS Versions prior to 1.13.0 Latitude 7340 BIOS Versions prior to 1.13.0 OptiPlex Micro 7010 / OptiPlex Micro Plus 7010 BIOS Versions prior to 1.13.1 OptiPlex Small Form Factor 7010 / OptiPlex Small Form Factor Plus 7010 BIOS Versions prior to 1.13.1 OptiPlex Tower 7010 / OptiPlex Tower Plus 7010 BIOS Versions prior to 1.13.1 Dell G15 5530 BIOS Versions prior to 1.14.0 Dell G16 7630 BIOS Versions prior to 1.14.0 Inspiron 13 5330 BIOS Versions prior to 1.14.0 XPS 9315 2-in-1 BIOS Versions prior to 1.15.0 Alienware m16 R1 BIOS Versions prior to 1.16.0 Alienware m18 R1 BIOS Versions prior to 1.16.0 PowerEdge T40 BIOS Versions prior to 1.16.0 Latitude 9330 BIOS Versions prior to 1.19.0 Latitude 5330 BIOS Versions prior to 1.21.0 Latitude 5531 BIOS Versions prior to 1.22.0 Latitude 9430 BIOS Versions prior to 1.22.0 Precision 3571 BIOS Versions prior to 1.22.0 Precision 5570 BIOS Versions prior to 1.22.0 Latitude 5310 BIOS Versions prior to 1.23.0 Latitude 5310 2-in-1 BIOS Versions prior to 1.23.0 Precision 5770 BIOS Versions prior to 1.24.0 XPS 17 9720 BIOS Versions prior to 1.24.0 Precision 3440 BIOS Versions prior to 1.25.0 Vostro 5880 BIOS Versions prior to 1.25.0 Inspiron 5400/5401 BIOS Versions prior to 1.27.0 Inspiron 5401 AIO BIOS Versions prior to 1.27.0 Inspiron 7700 All-In-One BIOS Versions prior to 1.27.0 Dell G15 5511 BIOS Versions prior to 1.28.0 Alienware m15 R6 BIOS Versions prior to 1.29.0 Dell G3 3500 BIOS Versions prior to 1.29.0 Dell G5 5500 BIOS Versions prior to 1.29.0 Inspiron 5402 BIOS Versions prior to 1.29.0 Inspiron 5409 BIOS Versions prior to 1.29.0 Inspiron 5502 BIOS Versions prior to 1.29.0 Inspiron 5509 BIOS Versions prior to 1.29.0 Latitude 9420 BIOS Versions prior to 1.29.0 Precision 5750 BIOS Versions prior to 1.29.0 Vostro 5402 BIOS Versions prior to 1.29.0 Vostro 5502 BIOS Versions prior to 1.29.0 XPS 17 9700 BIOS Versions prior to 1.29.0 Inspiron 3030S BIOS Versions prior to 1.3.0 Vostro 3030S BIOS Versions prior to 1.3.0 Dell G7 7500 BIOS Versions prior to 1.31.0 Dell G7 7700 BIOS Versions prior to 1.31.0 Inspiron 5301 BIOS Versions prior to 1.32.0 Inspiron 7300 BIOS Versions prior to 1.32.0 Inspiron 7400 BIOS Versions prior to 1.32.0 Vostro 5301 BIOS Versions prior to 1.32.0 Latitude 7320 BIOS Versions prior to 1.34.2 Latitude 7420 BIOS Versions prior to 1.34.2 Latitude 7520 BIOS Versions prior to 1.34.2 Precision 3660 BIOS Versions prior to 2.13.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000223962/dsa-2024-167-security-update-for-dell-poweredge-t30-t40-mini-tower-server-for-an-improper-input-validation-vulnerability • https://www.dell.com/support/kbdoc/en-us/000221744/dsa-2024-066 • https://www.dell.com/support/kbdoc/en-us/000216151/dsa-2023-272

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.