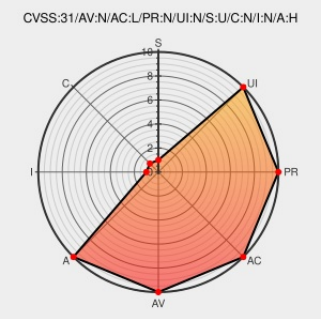
CVE-2022-25622

Published on: Not Yet Published

Last Modified on: 01/10/2023 12:15:00 PM UTC

CVE-2022-25622

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Simatic Cfu Diq from Siemens contain the following vulnerability:

A vulnerability has been identified in SIMATIC CFU DIQ (All versions), SIMATIC CFU PA (All versions), SIMATIC ET 200pro IM154-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200pro IM154-8FX PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIMATIC ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIMATIC ET200AL IM157-1 PN (All versions), SIMATIC ET200ecoPN, CM 8x IO-Link, M12-L (All versions >= V5.1.1), SIMATIC ET200ecoPN, DI 16x24VDC, M12-L (All versions >= V5.1.1), SIMATIC ET200ecoPN, DI 8x24VDC, M12-L (All versions >= V5.1.1), SIMATIC ET200ecoPN, DIQ 16x24VDC/2A, M12-L (All versions >= V5.1.1), SIMATIC ET200ecoPN, DQ 8x24VDC/0,5A, M12-L (All versions >= V5.1.1), SIMATIC ET200ecoPN, DQ 8x24VDC/2A, M12-L (All versions >= V5.1.1), SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants) (All versions >= V4.2), SIMATIC ET200SP IM155-6 MF HF (All versions), SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants) (All versions), SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants) (All versions >= V4.2), SIMATIC ET200SP IM155-6 PN/2 HF (incl. SIPLUS variants) (All versions >= V4.2), SIMATIC ET200SP IM155-6 PN/3 HF (incl. SIPLUS variants) (All versions >= V4.2), SIMATIC PN/MF Coupler (All versions), SIMATIC PN/PN Coupler (All versions >= 4.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.0.0), SIMATIC S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIMATIC S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 315T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317T-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 317TF-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319-3 PN/DP (All versions < V3.2.19), SIMATIC S7-300 CPU 319F-3 PN/DP (All versions < V3.2.19), SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants) (All versions < V6.0.10), SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) (All versions), SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants) (All versions < V10.1.1), SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants) (All versions < V8.2.3), SIMATIC TDC CP51M1 (All versions < V1.1.10), SIMATIC TDC CPU555 (All versions <

V1.2.1), SIMATIC WinAC RTX 2010 (All versions), SIMATIC WinAC RTX F 2010 (All versions), SINAMICS DCM (All versions with Ethernet interface), SINAMICS G110M (All versions with Ethernet interface), SINAMICS G115D (All versions with Ethernet interface), SINAMICS G120 (incl. SIPLUS variants) (All versions with Ethernet interface), SINAMICS G130 (All versions), SINAMICS G150 (All versions), SINAMICS S110 (All versions with Ethernet interface), SINAMICS S120 (incl. SIPLUS variants) (All versions < V5.2 SP3 HF13), SINAMICS S150 (All versions), SINAMICS S210 (All versions), SINAMICS V90 (All versions with Ethernet interface), SIPLUS ET 200S IM151-8 PN/DP CPU (All versions < V3.2.19), SIPLUS ET 200S IM151-8F PN/DP CPU (All versions < V3.2.19), SIPLUS HCS4200 CIM4210 (All versions), SIPLUS HCS4200 CIM4210C (All versions), SIPLUS HCS4300 CIM4310 (All versions), SIPLUS NET PN/PN Coupler (All versions >= 4.2), SIPLUS S7-300 CPU 314C-2 PN/DP (All versions < V3.3.19), SIPLUS S7-300 CPU 315-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 315F-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317-2 PN/DP (All versions < V3.2.19), SIPLUS S7-300 CPU 317F-2 PN/DP (All versions < V3.2.19). The PROFINET (PNIO) stack, when integrated with the Interniche IP stack, improperly handles internal resources for TCP segments where the minimum TCP-Header length is less than defined. This could allow an attacker to create a denial of service condition for TCP services on affected devices by sending specially crafted TCP segments.

CVE-2022-25622 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-446448.pdf

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

591199 Siemens PROFINET Stack Integrated on Interniche Stack (Update D) Vulnerability (ICSA-22-104-06, SSA-446448)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Simatic Cfu Diq	-	All	All	All
Operating System	Siemens	Simatic Cfu Diq Firmware	All	All	All	All
Hardware	Siemens	Simatic Cfu Pa	-	All	All	All
Operating System	Siemens	Simatic Cfu Pa Firmware	All	All	All	All
Hardware	Siemens	Simatic S7-1500 Cpu	-	All	All	All
Operating System	Siemens	Simatic S7-1500 Cpu Firmware	All	All	All	All
Hardware	Siemens	Simatic S7-300 Cpu	-	All	All	All
Operating System	Siemens	Simatic S7-300 Cpu Firmware	All	All	All	All
Hardware	Siemens	Simatic S7-400h V6	-	All	All	All
Operating System	Siemens	Simatic S7-400h V6 Firmware	All	All	All	All
Hardware	Siemens	Simatic S7-400 Pn/dp V7	-	All	All	All
Operating System	Siemens	Simatic S7-400 Pn/dp V7 Firmware	All	All	All	All
Hardware	Siemens	Simatic S7-410 V10	-	All	All	All
Operating System	Siemens	Simatic S7-410 V10 Firmware	All	All	All	All
Hardware	Siemens	Simatic S7-410 V8	-	All	All	All
Operating System	Siemens	Simatic S7-410 V8 Firmware	All	All	All	All
Hardware	Siemens	Simatic Tdc Cp51m1	-	All	All	All
Operating System	Siemens	Simatic Tdc Cp51m1 Firmware	All	All	All	All
Hardware	Siemens	Simatic Tdc Cpu555	-	All	All	All
Operating System	Siemens	Simatic Tdc Cpu555 Firmware	All	All	All	All
Hardware	Siemens	Simatic Winac Rtx	-	All	All	All

Operating System	Siemens	Simatic Winac Rtx Firmware	All	All	All	All
Application	Siemens	Simit Simulation Platform	All	All	All	All

cpe:2.3:h:siemens:simatic_cfu_diq:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cfu_diq_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_cfu_pa:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_cfu_pa_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_s7-1500_cpu:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_s7-1500_cpu_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_s7-300_cpu:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_s7-300_cpu_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_s7-400h_v6:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_s7-400h_v6_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_s7-400_pn\/dp_v7:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_s7-400_pn\/dp_v7_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_s7-410_v10:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_s7-410_v10_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_s7-410_v8:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_s7-410_v8_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_tdc_cp51m1:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_tdc_cp51m1_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_tdc_cpu555:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_tdc_cpu555_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_winac_rtx:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_winac_rtx_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:a:siemens:simit_simulation_platform:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-25622 : A vulnerability has been identified in SIMATIC CFU DIQ All versions , SIMATIC CFU PA All version… twitter.com/i/web/status/1…	2022-04-12 09:13:35
/r/netcve	CVE-2022-25622	2022-04-12 10:38:49

← Previous ID

Next ID→