	A	B	C	D	E	F	G	H	I	J
1	**No.**	**CVE ID**	Description	**CVSS v3 Score**	**Vector**	**Vendor**	**Device**	**Hardware/CPU**	**Firmware version**	**Note**
2	1	CVE-2021-44695	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	4.9	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
3	2	CVE-2021-44694	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	5.5	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
4	3	CVE-2021-44693	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	4.9	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
5	4	CVE-2021-40365	Affected devices don't process correctly certain special crafted packets sent to port 102/tcp, which could allow an attacker to cause a denial of service in the device.	7.5	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
6	5	CVE-2021-37205	A vulnerability has been identified in SIMATIC Drive Controller family (All versions >= V2.9.2 < V2.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V21.9 < V21.9.4), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions >= V4.5.0 < V4.5.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.9.2 < V2.9.4), SIMATIC S7-1500 Software Controller (All versions >= V21.9 < V21.9.4), SIMATIC S7-PLCSIM Advanced (All versions >= V4.0 < V4.0 SP1), SIPLUS TIM 1531 IRC (All versions < V2.3.6), TIM 1531 IRC (All versions < V2.3.6). An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.	7.1	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
7	6	CVE-2021-37204	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC Drive Controller family (All versions >= V2.9.2 < V2.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V21.9 < V21.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 Ready4Linux (All versions), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions >= V4.5.0 < V4.5.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.9.2 < V2.9.4), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-1500 Software Controller (All versions >= V21.9 < V21.9.4), SIMATIC S7-PLCSIM Advanced (All versions < V4.0), SIMATIC S7-PLCSIM Advanced (All versions >= V4.0 < V4.0 SP1), SIPLUS TIM 1531 IRC (All versions < V2.3.6), TIM 1531 IRC (All versions < V2.3.6). An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packet over port 102/tcp. A restart of the affected device is needed to restore normal operations.	7.1	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	

	A	B	C	D	E	F	G	H	I	J
8	7	CVE-2021-37185	A vulnerability has been identified in SIMATIC Drive Controller family (All versions >= V2.9.2 < V2.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V21.9 < V21.9.4), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions >= V4.5.0 < V4.5.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.9.2 < V2.9.4), SIMATIC S7-1500 Software Controller (All versions >= V21.9 < V21.9.4), SIMATIC S7-PLCSIM Advanced (All versions >= V4.0 < V4.0 SP1), SIPLUS TIM 1531 IRC (All versions < V2.3.6), TIM 1531 IRC (All versions < V2.3.6). An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.	7.1	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
9	8	CVE-2022-30694	The login endpoint /FormLogin in affected web services does not apply proper origin checking. This could allow authenticated remote attackers to track the activities of other users via a login cross-site request forgery attack.	6.5	Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
10	9	CVE-2021-3449	An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).	5.9	Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
11	10	CVE-2019-10936	A vulnerability has been identified in SIMATIC S7-400 CPU 414-3 PN/DP V7, SIMATIC S7-400 CPU 414F-3 PN/DP V7, SIMATIC S7-400 CPU 416-3 PN/DP V7, SIMATIC S7-400 CPU 416F-3 PN/DP V7, Development/Evaluation Kits for PROFINET IO: DK Standard Ethernet Controller, Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200, Development/Evaluation Kits for PROFINET IO: EK-ERTEC 200P, SIMATIC CFU PA, SIMATIC ET 200pro IM154-8 PN/DP CPU, SIMATIC ET 200pro IM154-8F PN/DP CPU, SIMATIC ET 200pro IM154-8FX PN/DP CPU, SIMATIC ET 200S IM151-8 PN/DP CPU, SIMATIC ET 200S IM151-8F PN/DP CPU, SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants), SIMATIC ET200AL, SIMATIC ET200ecoPN, 16DI, DC24V, 8xM12, SIMATIC ET200ecoPN, 16DO DC24V/1,3A, 8xM12, SIMATIC ET200ecoPN, 4AO U/I 4xM12, SIMATIC ET200ecoPN, 8 DIO, DC24V/1,3A, 8xM12, SIMATIC ET200ecoPN, 8 DO, DC24V/2A, 8xM12, SIMATIC ET200ecoPN, 8AI RTD/TC 8xM12, SIMATIC ET200ecoPN, 8AI; 4 U/I; 4 RTD/TC 8xM12, SIMATIC ET200ecoPN, 8DI, DC24V, 4xM12, SIMATIC ET200ecoPN, 8DI, DC24V, 8xM12, SIMATIC ET200ecoPN, 8DO, DC24V/0,5A, 4xM12, SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 4xM12, SIMATIC ET200ecoPN, 8DO, DC24V/1,3A, 8xM12, SIMATIC ET200ecoPN: IO-Link Master, SIMATIC ET200M (incl. SIPLUS variants), SIMATIC ET200MP IM155-5 PN BA (incl. SIPLUS variants), SIMATIC ET200MP IM155-5 PN HF (incl. SIPLUS variants), SIMATIC ET200MP IM155-5 PN ST (incl. SIPLUS variants), SIMATIC ET200pro, SIMATIC ET200S (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN BA (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN HA (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN HF (incl. SIPLUS variants), SIMATIC ET200SP IM155-6 PN HS (incl. SIPLUS variants), SIMATIC ET200SP	7.5		Siemens	PLC S7-1200	CPU 1212C	4.5.1	

	A	B	C	D	E	F	G	H	I	J
12	11	**CVE-2019-10943**	A vulnerability has been identified in SIMATIC Drive Controller family (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V20.8), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V20.8), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.4.0), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions >= V4.4.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.8.1), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.8.1), SIMATIC S7-1500 Software Controller (All versions < V20.8), SIMATIC S7-1500 Software Controller (All versions >= V20.8), SIMATIC S7-PLCSIM Advanced (All versions < V3.0), SIMATIC S7-PLCSIM Advanced (All versions >= V3.0). An attacker with network access to port 102/tcp could potentially modify the user program on the PLC in a way that the running code is different from the source code which is stored on the device. An attacker must have network access to affected devices and must be able to perform changes to the user program. The vulnerability could impact the perceived integrity of the user program stored on the CPU. An engineer that tries to obtain the code of the user program running on the device, can receive different source code that is not actually running on the device.	7.5	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
13	12	CVE-2019-10929	A vulnerability has been identified in SIMATIC CP 1626 (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V20.8), SIMATIC HMI Panel (incl. SIPLUS variants) (All versions), SIMATIC NET PC Software V14 (All versions < V14 SP1 Update 14), SIMATIC NET PC Software V15 (All versions), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.4.0), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.8.1), SIMATIC S7-1500 Software Controller (All versions < V20.8), SIMATIC S7-PLCSIM Advanced (All versions < V3.0), SIMATIC STEP 7 (TIA Portal) (All versions < V16), SIMATIC WinCC (TIA Portal) (All versions < V16), SIMATIC WinCC OA (All versions < V3.16 P013), SIMATIC WinCC Runtime Advanced (All versions < V16), SIMATIC WinCC Runtime Professional (All versions < V16), TIM 1531 IRC (incl. SIPLUS NET variants) (All versions < V2.1). Affected devices contain a message protection bypass vulnerability due to certain properties in the calculation used for integrity protection. This could allow an attacker in a Man-in-the-Middle position to modify network traffic sent on port 102/tcp to the affected devices.	5.9	Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N	Siemens	PLC S7-1200	CPU 1212C	4.5.1	
14	13	CVE-2023-0286	There is a type confusion vulnerability relating to X.400 address processing inside an X.509 GeneralName. X.400 addresses were parsed as an ASN1_STRING but the public structure definition for GENERAL_NAME incorrectly specified the type of the x400Address	7.4		Siemens	PLC S7-1200	CPU 1212C	4.5.1	
15	14	CVE-2023-37482	The login functionality of the web server in affected devices does not normalize the response times of login attempts. An unauthenticated remote attacker could exploit this side-channel information to distinguish between valid and invalid usernames.	6.9		Siemens	PLC S7-1200	CPU 1212C	4.5.1	

	A	B	C	D	E	F	G	H	I	J
16	15	CVE-2024-46886	The web server of affected devices does not properly validate input that is used for a user redirection. This could allow an attacker to make the server redirect the legitimate user to an attacker-chosen URL. For a successful exploit, the legitimate user	5.1		Siemens	PLC S7-1200	CPU 1212C	4.5.1	
17	16	CVE-2024-47100	A vulnerability has been identified in SIMATIC S7-1200 CPU 1211C AC/DC/Rly (6ES7211-1BE40-0XB0), SIMATIC S7-1200 CPU 1211C DC/DC/DC (6ES7211-1AE40-0XB0), SIMATIC S7-1200 CPU 1211C DC/DC/Rly (6ES7211-1HE40-0XB0), SIMATIC S7-1200 CPU 1212C AC/DC/Rly (6ES721	7.2		Siemens	PLC S7-1200	CPU 1212C	4.5.1	
18	17	CVE-2025-24811	A vulnerability has been identified in SIMATIC S7-1200 CPU 1211C AC/DC/Rly (6ES7211-1BE40-0XB0), SIMATIC S7-1200 CPU 1211C DC/DC/DC (6ES7211-1AE40-0XB0), SIMATIC S7-1200 CPU 1211C DC/DC/Rly (6ES7211-1HE40-0XB0), SIMATIC S7-1200 CPU 1212C AC/DC/Rly (6ES721	8.7		Siemens	PLC S7-1200	CPU 1212C	4.5.1	
19	18	CVE-2025-24812	A vulnerability has been identified in SIMATIC S7-1200 CPU 1211C AC/DC/Rly (6ES7211-1BE40-0XB0) (All versions < V4.7), SIMATIC S7-1200 CPU 1211C DC/DC/DC (6ES7211-1AE40-0XB0) (All versions < V4.7), SIMATIC S7-1200 CPU 1211C DC/DC/Rly (6ES7211-1HE40-0XB0)	7.1		Siemens	PLC S7-1200	CPU 1212C	4.5.1	
20	19	CVE-2021-22699	Improper Input Validation vulnerability exists in Modicon M241/M251 logic controllers firmware prior to V5.1.9.1 that could cause denial of service when specific crafted requests are sent to the controller over HTTP.	7.5	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	Schneider Electric	Modicon M241		05.0.8.7	
21	20	CVE-2020-7488	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers.	7.5	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Schneider Electric	Modicon M241		05.0.8.7	
22	21	CVE-2020-7487	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers.	9.8	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Schneider Electric	Modicon M241		05.0.8.7	
23	22	CVE-2019-6820	A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received in all versions of: Modicon M100, Modicon M200, Modicon M221, ATV IMC drive controller, Modicon M241, Modicon M251, Modicon M258, Modicon LMC058, Modicon LMC078, PacDrive Eco ,PacDrive Pro, PacDrive Pro2	8.2	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H	Schneider Electric	Modicon M241		05.0.8.7	
24	23	CVE-2017-6030	A Predictable Value Range from Previous Values issue was discovered in Schneider Electric Modicon PLCs Modicon M221, firmware versions prior to Version 1.5.0.0, Modicon M241, firmware versions prior to Version 4.0.5.11, and Modicon M251, firmware versions prior to Version 4.0.5.11. The affected products generate insufficiently random TCP initial sequence numbers that may allow an attacker to predict the numbers from previous values. This may allow an attacker to spoof or disrupt TCP connections.	6.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L	Schneider Electric	Modicon M241		05.0.8.7	
25	24	CVE-2017-6026	A Use of Insufficiently Random Values issue was discovered in Schneider Electric Modicon PLCs Modicon M241, firmware versions prior to Version 4.0.5.11, and Modicon M251, firmware versions prior to Version 4.0.5.11. The session numbers generated by the web application are lacking randomization and are shared between several users. This may allow a current session to be compromised.	9.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	Schneider Electric	Modicon M241		05.0.8.7	

	A	B	C	D	E	F	G	H	I	J
26	25	CVE-2017-6028	An Insufficiently Protected Credentials issue was discovered in Schneider Electric Modicon PLCs Modicon M241, all firmware versions, and Modicon M251, all firmware versions. Log-in credentials are sent over the network with Base64 encoding leaving them susceptible to sniffing. Sniffed credentials could then be used to log into the web application.	9.8	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Schneider Electric	Modicon M241		05.0.8.7	
27	26	CVE-2020-6980	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, If Simple Mail Transfer Protocol (SMTP) account data is saved in RSLogix 500, a local attacker with access to a victim's project may be able to gather SMTP server authentication data as it is written to the project file in cleartext.	3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N	Rockwell Automation	MicroLogix 1400	1766-L32BXB	1.5.0	
28	27	CVE-2020-6988	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, A remote, unauthenticated attacker can send a request from the RSLogix 500 software to the victim's MicroLogix controller. The controller will then respond to the client with used password values to authenticate the user on the client-side. This method of authentication may allow an attacker to bypass authentication altogether, disclose sensitive information, or leak credentials.	7.5	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Rockwell Automation	MicroLogix 1400	1766-L32BXB	1.5.0	
29	28	CVE-2020-6984	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic function utilized to protect the password in MicroLogix is discoverable.	7.5	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Rockwell Automation	MicroLogix 1400	1766-L32BXB	1.5.0	
30	29	CVE-2020-6990	Rockwell Automation MicroLogix 1400 Controllers Series B v21.001 and prior, Series A, all versions, MicroLogix 1100 Controller, all versions, RSLogix 500 Software v12.001 and prior, The cryptographic key utilized to help protect the account password is hard coded into the RSLogix 500 binary file. An attacker could identify cryptographic keys and use it for further cryptographic attacks that could ultimately lead to a remote attacker gaining unauthorized access to the controller.	9.8	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	Rockwell Automation	MicroLogix 1400	1766-L32BXB	1.5.0	
31	30	**CVE-2019-10955**	In Rockwell Automation MicroLogix 1400 Controllers Series A, All Versions Series B, v15.002 and earlier, MicroLogix 1100 Controllers v14.00 and earlier, CompactLogix 5370 L1 controllers v30.014 and earlier, CompactLogix 5370 L2 controllers v30.014 and earlier, CompactLogix 5370 L3 controllers (includes CompactLogix GuardLogix controllers) v30.014 and earlier, an open redirect vulnerability could allow a remote unauthenticated attacker to input a malicious link to redirect users to a malicious site that could run or download arbitrary malware on the user's machine.	6.1	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	Rockwell Automation	MicroLogix 1400	1766-L32BXB	1.5.0	
32	31	CVE-2023-0457	Plaintext Storage of a Password vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series, MELSEC iQ-R Series, MELSEC-Q Series and MELSEC-L Series allows a remote unauthenticated attacker to disclose plaintext credentials stored in project files and login into FTP server or Web server.	7.5	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	Mitsubishi PLC		FX5UC 64MT/D	1.074	

	A	B	C	D	E	F	G	H	I	J
33	32	CVE-2022-40267	Predictable Seed in Pseudo-Random Number Generator (PRNG) vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U-xMy/z (x=32,64,80, y=T,R, z=ES,DS,ESS,DSS) with serial number 17X**** or later, and versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5U-xMy/z (x=32,64,80, y=T,R, z=ES,DS,ESS,DSS) with serial number 179**** and prior, and versions 1.074 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-xMy/z (x=32,64,96, y=T, z=D,DSS)) with serial number 17X**** or later, and versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-xMy/z (x=32,64,96, y=T, z=D,DSS)) with serial number 179**** and prior, and versions 1.074 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-32MT/DS-TS versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-32MT/DSS-TS versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UJ-xMy/z (x=24,40,60, y=T,R, z=ES,ESS) versions 1.042 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UJ-xMy/ES-A (x=24,40,60, y=T,R) versions 1.043 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5S-xMy/z (x=30,40,60,80, y=T,R, z=ES,ESS) versions 1.003 and prior, Mitsubishi Electric Corporation MELSEC iQ-F Series FX5UC-32MR/DS-TS versions 1.280 and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R00/01/02CPU versions 33 and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R04/08/16/32/120(EN)CPU versions 66 and prior allows a remote unauthenticated attacker to access the Web server function by guessing the random numbers used for authentication from several used random numbers.	9.1	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N	Mitsubishi PLC		FX5UC 64MT/D	1.074	
34	33	CVE-2023-4625	Improper Restriction of Excessive Authentication Attempts vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F/iQ-R Series CPU modules Web server function allows a remote unauthenticated attacker to prevent legitimate users from logging into the Web server function for a certain period after the attacker has attempted to log in illegally by continuously attempting unauthorized login to the Web server function. The impact of this vulnerability will persist while the attacker continues to attempt unauthorized login.	5.3	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L	Mitsubishi PLC		FX5UC 64MT/D	1.074	
35	34	CVE-2023-4699	Insufficient Verification of Data Authenticity vulnerability in Mitsubishi Electric Corporation MELSEC-F Series main modules and MELSEC iQ-F Series CPU modules allows a remote unauthenticated attacker to reset the memory of the products to factory default state and cause denial-of-service (DoS) condition on the products by sending specific packets.	9.1	Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	Mitsubishi PLC		FX5UC 64MT/D	1.074	