PEPPERL+FUCHS Your automation, our passion.

CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Device Master ICDM-RX/* – Vulnerability may allow attackers to interact with a user via dialog box

VDE-ID VDE-2024-033
Document-ID TDOCT-9401AENG
Publication date 2024-08-13

Vulnerabilities

Identifier	Vulnerability Type	Description
CVE-2024-38501	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	An unauthenticated remote attacker may use a HTML injection vulnerability with limited length to inject malicious HTML code and gain low-privileged access on the affected device.
CVE-2024-5849	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	An unauthenticated remote attacker may use a reflected XSS vulnerability to obtain information from a user or reboot the affected device once.
CVE-2024-38502	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	An unauthenticated remote attacker may use stored XSS vulnerability to obtain information from a user or reboot the affected device once.

Severity

Identifier	Base Score and Vector
CVE-2024-38501	6.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N)
CVE-2024-5849	7.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L)
CVE-2024-38502	7.1 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:L)

Affected products

Item No.	Item	Version
70104867	ICDM-RX/TCP-DB9/RJ45-DIN	SocketServer 11.65 or older
70104868	ICDM-RX/TCP-ST/RJ45-DIN	SocketServer 11.65 or older
70104869	ICDM-RX/TCP-4DB9/2RJ45-DIN	SocketServer 11.65 or older
70104885	ICDM-RX/TCP-DB9/RJ45-PM	SocketServer 11.65 or older
70114044	ICDM-RX/TCP-2DB9/RJ45-DIN	SocketServer 11.65 or older
70114045	ICDM-RX/TCP-2ST/RJ45-DIN	SocketServer 11.65 or older
70114046	ICDM-RX/TCP-4DB9/2RJ45-PM	SocketServer 11.65 or older
70114047	ICDM-RX/TCP-8DB9/2RJ45-PM	SocketServer 11.65 or older
70114048	ICDM-RX/TCP-16RJ45/RJ45-RM	SocketServer 11.65 or older

70114049	ICDM-RX/TCP-16DB9/RJ45-RM	SocketServer 11.65 or older
70114050	ICDM-RX/TCP-32RJ45/RJ45-RM	SocketServer 11.65 or older
70139038	ICDM-RX/TCP-DB9/RJ45-PM2	SocketServer 11.65 or older
70139042	ICDM-RX/TCP-16RJ45/2RJ45-PM	SocketServer 11.65 or older
70104873	ICDM-RX/PN-DB9/RJ45-DIN	PROFINET v3.4.9 or older
70104874	ICDM-RX/PN-ST/RJ45-DIN	PROFINET v3.4.9 or older
70104875	ICDM-RX/PN-4DB9/2RJ45-DIN	PROFINET v3.4.9 or older
70114018	ICDM-RX/PN-DB9/RJ45-PM	PROFINET v3.4.9 or older
70114028	ICDM-RX/PN-2DB9/RJ45-DIN	PROFINET v3.4.9 or older
70114029	ICDM-RX/PN-2ST/RJ45-DIN	PROFINET v3.4.9 or older
70114025	ICDM-RX/PN1-DB9/RJ45-PM	PROFINET/Modbus v1.0.7 or older
70114037	ICDM-RX/PN1-DB9/RJ45-DIN	PROFINET/Modbus v1.0.7 or older
70114038	ICDM-RX/PN1-ST/RJ45-DIN	PROFINET/Modbus v1.0.7 or older
70114039	ICDM-RX/PN1-2DB9/RJ45-DIN	PROFINET/Modbus v1.0.7 or older
70114040	ICDM-RX/PN1-4DB9/2RJ45-DIN	PROFINET/Modbus v1.0.7 or older
70114042	ICDM-RX/PN1-2ST/RJ45-DIN	PROFINET/Modbus v1.0.7 or older
70104870	ICDM-RX/EN-DB9/RJ45-DIN	EtherNet/IP v7.22 or older
70104871	ICDM-RX/EN-ST/RJ45-DIN	EtherNet/IP v7.22 or older
70104872	ICDM-RX/EN-4DB9/2RJ45-DIN	EtherNet/IP v7.22 or older
70114020	ICDM-RX/EN-DB9/RJ45-PM	EtherNet/IP v7.22 or older
70114026	ICDM-RX/EN-2DB9/RJ45-DIN	EtherNet/IP v7.22 or older
70114027	ICDM-RX/EN-2ST/RJ45-DIN	EtherNet/IP v7.22 or older
70114024	ICDM-RX/EN1-DB9/RJ45-PM	EIP/Modbus v1.08 or older
70114032	ICDM-RX/EN1-DB9/RJ45-DIN	EIP/Modbus v1.08 or older
70114033	ICDM-RX/EN1-ST/RJ45-DIN	EIP/Modbus v1.08 or older
70114034	ICDM-RX/EN1-2DB9/RJ45-DIN	EIP/Modbus v1.08 or older
70114035	ICDM-RX/EN1-4DB9/2RJ45-DIN	EIP/Modbus v1.08 or older
70114036	ICDM-RX/EN1-2ST/RJ45-DIN	EIP/Modbus v1.08 or older
70104882	ICDM-RX/MOD-DB9/RJ45-DIN	Modbus Router v7.09 or older Modbus Server v7.11 or older Modbus TCP v7.11 or older
70104883	ICDM-RX/MOD-ST/RJ45-DIN	Modbus Router v7.09 or older Modbus Server v7.11 or older Modbus TCP v7.11 or older
70104884	ICDM-RX/MOD-4DB9/2RJ45-DIN	Modbus Router v7.09 or older Modbus Server v7.11 or older Modbus TCP v7.11 or older
70114021	ICDM-RX/MOD-DB9/RJ45-PM	Modbus Router v7.09 or older Modbus Server v7.11 or older

		Modbus TCP v7.11 or older
70114030	ICDM-RX/MOD-2DB9/RJ45-DIN	Modbus Router v7.09 or older Modbus Server v7.11 or older Modbus TCP v7.11 or older
70114031	ICDM-RX/MOD-2ST/RJ45-DIN	Modbus Router v7.09 or older Modbus Server v7.11 or older Modbus TCP v7.11 or older
70139043	ICDM-RX/MOD-16RJ45/2RJ45-PM	Modbus Router v7.09 or older Modbus Server v7.11 or older Modbus TCP v7.11 or older

Summary

Vulnerabilities has been discovered in the product, mainly caused by HTML injection and crosssite-scripting.

The impact of the vulnerability on the affected device may result in an information disclosure and denial of service.

Impact

An unauthenticated remote attacker may use

- a HTML injection vulnerability with limited length to inject malicious HTML code.
- a reflected XSS vulnerability to obtain information from a user or reboot the device once.
- stored XSS vulnerability to obtain information from a user or reboot the device once.

Solution

Update to a new version of the firmware you are using:

- SocketServer v11.66
- PROFINET v3.4.10
- PROFINET/Modbus v1.0.8
- EtherNet/IP v7.23
- EIP/Modbus v1.09
- Modbus Router v7.10
- Modbus Server v7.12
- Modbus TCP v7.12

Reported by

Christopher Di-Nozzi
Pepperl + Fuchs SE
Coordinated by CERT@VDE

Support

For support please contact your local Pepperl+Fuchs sales representative.