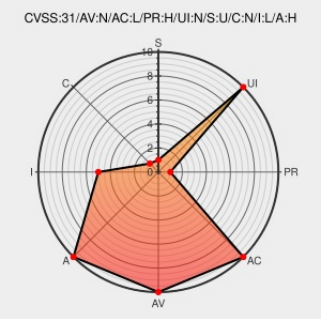
CVE-2022-34765

Published on: Not Yet Published

Last Modified on: 07/21/2022 07:54:00 PM UTC

CVE-2022-34765

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



Certain versions of Opc Ua Module For M580 from Schneider-electric contain the following vulnerability:

A CWE-73: External Control of File Name or Path vulnerability exists that could cause loading of unauthorized firmware images when user-controlled data is written to the file path. Affected Products: X80 advanced RTU Communication Module (BMENOR2200H) (V2.01 and later), OPC UA Modicon Communication Module (BMENUA0100) (V1.10 and prior)

CVE-2022-34765 has been assigned by cybersecurity@schneider-electric.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **Schneider Electric** - **OPC UA Modicon Communication Module** version **< V1.10**

Affected Vendor/Software: **Schneider Electric** - **X80 advanced RTU Communication Module** version **> V2.01**

CVSS3 Score: 5.3 - MEDIUM

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

CVE References

Description	Tags	Link
	download.schneider-electric.com application/pdf Inactive Link Not Archived	MISC download.schneider-electric.com/files?p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-193-01_OPC_UA_X80_Advanced_RTU_Modicon_Communication_Modules+_Security_Notificatio

comment@cve.report.

Related QID Numbers

590966 Schneider Electric OPC UA and X80 Advanced RTU Modicon Communication Modules Multiple Vulnerabilities (SEVD-2022-193-01)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Schneider-electric	Opc Ua Module For M580	-	All	All	All
Operating System	Schneider-electric	Opc Ua Module For M580 Firmware	All	All	All	All
Hardware	Schneider-electric	X80 Advanced Rtu Module	-	All	All	All
Operating System	Schneider-electric	X80 Advanced Rtu Module Firmware	All	All	All	All

cpe:2.3:h:schneider-electric:opc_ua_module_for_m580:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:opc_ua_module_for_m580_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:x80_advanced_rtu_module:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:x80_advanced_rtu_module_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-34765 : A CWE-73: External Control of File Name or Path vulnerability exists that could cause loading of u… twitter.com/i/web/status/1…	2022-07-13 21:20:35
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-34765 A CWE-73: External Control of File Name or Path vulnerability exi… twitter.com/i/web/status/1…	2022-07-13 23:55:58
@threatmeter	CVE-2022-34765 | Schneider Electric X80 Advanced RTU Communication Module Firmware Image file inclusion (SEVD-2022-… twitter.com/i/web/status/1…	2022-07-14 07:50:50
@ColorTokensInc	Emerging Vulnerability Found CVE-2022-34765 - A CWE-73: External Control of File Name or Path vulnerability exists… twitter.com/i/web/status/1…	2022-07-14 07:50:56
/r/netcve	CVE-2022-34765	2022-07-13 21:39:08

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report