



CVE-2021-37186

Published on: 09/14/2021 12:00:00 AM UTC

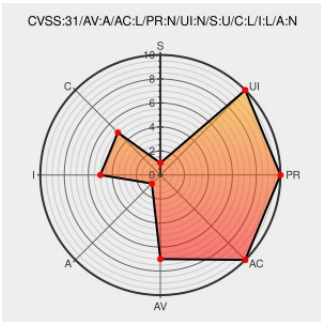
Last Modified on: 09/24/2021 01:48:00 PM UTC

CVE-2021-37186

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Logo! Cmr2020](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in LOGO! CMR2020 (All versions < V2.2), LOGO! CMR2040 (All versions < V2.2), SIMATIC RTU 3000 family (All versions). The underlying TCP/IP stack does not properly calculate the random numbers used as ISN (Initial Sequence Numbers). An adjacent attacker with network access to the LAN

interface could interfere with traffic, spoof the connection and gain access to sensitive information.

CVE-2021-37186 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [S](#) Siemens - LOGO! CMR2020 version All versions < V2.2

Affected Vendor/Software: [S](#) Siemens - LOGO! CMR2040 version All versions < V2.2

Affected Vendor/Software: [S](#) Siemens - SIMATIC RTU 3000 family version All versions

CVSS3 Score: **5.4 - MEDIUM**

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

CVSS2 Score: **4.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	S MISC cert-portal.siemens.com/productcert/pdf/ssa-316383.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that 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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Logo! Cmr2020	-	All	All	All
Operating System	Siemens	Logo! Cmr2020 Firmware	All	All	All	All
Hardware	Siemens	Logo! Cmr2040	-	All	All	All
Operating System	Siemens	Logo! Cmr2040 Firmware	All	All	All	All
Hardware	Siemens	Simatic Rtu3010c	All	All	All	All
Operating System	Siemens	Simatic Rtu3010c Firmware	-	All	All	All
Hardware	Siemens	Simatic Rtu3030c	All	All	All	All
Operating System	Siemens	Simatic Rtu3030c Firmware	-	All	All	All
Hardware	Siemens	Simatic Rtu3031c	All	All	All	All
Operating System	Siemens	Simatic Rtu3031c Firmware	-	All	All	All
Hardware	Siemens	Simatic Rtu3041c	All	All	All	All
Operating System	Siemens	Simatic Rtu3041c Firmware	-	All	All	All

cpe:2.3:h:siemens:logo!_cmr2020:-:~::~:~::~:~::~:~::~:~::~:

cpe:2.3:o:siemens:logo!_cmr2020_firmware:~::~:~::~:~::~:~::~:~::~:

cpe:2.3:h:siemens:logo!_cmr2040:-:~::~:~::~:~::~:~::~:~::~:

cpe:2.3:o:siemens:logo!_cmr2040_firmware:~::~:~::~:~::~:~::~:~::~:

cpe:2.3:h:siemens:simatic_rtu3010c:~::~:~::~:~::~:~::~:~::~:

cpe:2.3:o:siemens:simatic_rtu3010c_firmware:-:~::~:~::~:~::~:~::~:~::~:

cpe:2.3:h:siemens:simatic_rtu3030c:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_rtu3030c_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_rtu3031c:*:*:*:*:*:*:*:



cpe:2.3:o:siemens:simatic_rtu3031c_firmware:-:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:simatic_rtu3041c:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:simatic_rtu3041c_firmware:-:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-37186 : A vulnerability has been identified in LOGO! CMR2020 All versions < V2.2 , LOGO! CMR2040 All ver... twitter.com/i/web/status/1...	2021-09-14 11:00:55
 @threatmeter	CVE-2021-37186 A vulnerability has been identified in LOGO! CMR2020 (All versions < V2.2), LOGO! CMR2040 (All versi... twitter.com/i/web/status/1...	2021-09-15 07:09:34

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2021   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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