



CVE-2021-40368

Published on: Not Yet Published

Last Modified on: 08/10/2022 08:27:00 PM UTC

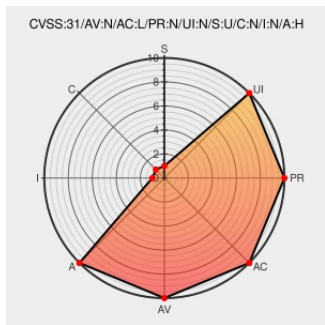
CVE-2021-40368

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Simatic S7-400h V6** from **Siemens** contain the following vulnerability:

A vulnerability has been identified in 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), SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants) (All versions < V8.2.3). Affected devices improperly handle specially crafted packets sent to port 102/tcp. This could allow an attacker to create a Denial-of-Service condition. A restart is needed to restore normal operations.

CVE-2021-40368 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Siemens** - **SIMATIC S7-400 H V6 CPU family (incl. SIPLUS variants)** version **All versions < V6.0.10**

Affected Vendor/Software: **Siemens** - **SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants)** version **All versions**

Affected Vendor/Software: **Siemens** - **SIMATIC S7-410 V10 CPU family (incl. SIPLUS variants)** version **All versions < V10.1**

Affected Vendor/Software: **Siemens** - **SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants)** version **All versions < V8.2.3**

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-557541.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.

Related QID Numbers

590853 Siemens SIMATIC S7-400 Vulnerability (icsa-22-104-12) (ssa-557541)



Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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
<pre>cpe:2.3:h:siemens:simatic_s7-400h_v6:-:*:*:*:*:*:</pre>						
<pre>cpe:2.3:o:siemens:simatic_s7-400h_v6_firmware:*:*:*:*:*:</pre>						
<pre>cpe:2.3:h:siemens:simatic_s7-400_pn\dp_v7:-:*:*:*:*:*:</pre>						
<pre>cpe:2.3:o:siemens:simatic_s7-400_pn\dp_v7_firmware:*:*:*:*:*:</pre>						
<pre>cpe:2.3:h:siemens:simatic_s7-410_v10:-:*:*:*:*:*:</pre>						
<pre>cpe:2.3:o:siemens:simatic_s7-410_v10_firmware:*:*:*:*:*:</pre>						
<pre>cpe:2.3:h:siemens:simatic_s7-410_v8:-:*:*:*:*:*:</pre>						

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVereport	CVE-2021-40368 : A vulnerability has been identified in SIMATIC S7-400 H V6 CPU family incl. SIPLUS variants All... twitter.com/i/web/status/1...	2022-04-12 09:20:35
 /r/netcve	CVE-2021-40368	2022-04-12 10:38:59

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2022   |

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](#)