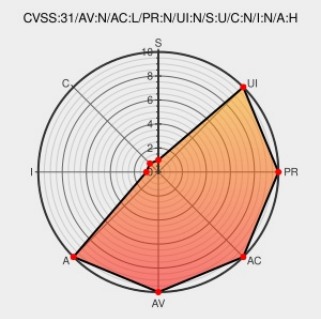
CVE-2022-46352

Published on: Not Yet Published

Last Modified on: 12/16/2022 02:43:00 PM UTC

CVE-2022-46352

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



Certain versions of 6gk5204-0ba00-2kb2 from Siemens contain the following vulnerability:

A vulnerability has been identified in SCALANCE X204RNA (HSR) (All versions < V3.2.7), SCALANCE X204RNA (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (HSR) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP) (All versions < V3.2.7), SCALANCE X204RNA EEC (PRP/HSR) (All versions < V3.2.7). Specially crafted PROFINET DCP packets could cause a denial of service condition of affected products.

CVE-2022-46352 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Siemens** - **SCALANCE X204RNA (HSR)** version **All versions < V3.2.7**

Affected Vendor/Software: **Siemens** - **SCALANCE X204RNA (PRP)** version **All versions < V3.2.7**

Affected Vendor/Software: **Siemens** - **SCALANCE X204RNA EEC (HSR)** version **All versions < V3.2.7**

Affected Vendor/Software: **Siemens** - **SCALANCE X204RNA EEC (PRP)** version **All versions < V3.2.7**

Affected Vendor/Software: **Siemens** - **SCALANCE X204RNA EEC (PRP/HSR)** version **All versions < V3.2.7**

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

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-363821.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

591279 Siemens SCALANCE X-200RNA Switch Devices Denial of Service (DoS), Hijacking of web sessions Multiple Vulnerabilities (ICSA-22-349-02, SSA-363821)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	6gk5204-0ba00-2kb2	-	All	All	All
Operating System	Siemens	6gk5204-0ba00-2kb2 Firmware	All	All	All	All
Hardware	Siemens	6gk5204-0ba00-2mb2	-	All	All	All
Operating System	Siemens	6gk5204-0ba00-2mb2 Firmware	All	All	All	All
Hardware	Siemens	6gk5204-0bs00-2na3	-	All	All	All
Operating System	Siemens	6gk5204-0bs00-2na3 Firmware	All	All	All	All
Hardware	Siemens	6gk5204-0bs00-3la3	-	All	All	All
Operating System	Siemens	6gk5204-0bs00-3la3 Firmware	All	All	All	All
Hardware	Siemens	6gk5204-0bs00-3pa3	-	All	All	All
Operating System	Siemens	6gk5204-0bs00-3pa3 Firmware	All	All	All	All

cpe:2.3:h:siemens:6gk5204-0ba00-2kb2:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6gk5204-0ba00-2kb2_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6gk5204-0ba00-2mb2:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6gk5204-0ba00-2mb2_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6gk5204-0bs00-2na3:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6gk5204-0bs00-2na3_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6gk5204-0bs00-3la3:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6gk5204-0bs00-3la3_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:6gk5204-0bs00-3pa3:-:*:*:*:*:*:*:*:

cpe:2.3:o:siemens:6gk5204-0bs00-3pa3_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	cve.report/CVE-2022-46352 A vulnerability has been identified in SCALANCE X204RNA HSR All versions < V3.2.7 ,… twitter.com/i/web/status/1…	2022-12-13 17:30:33
/r/netcve	CVE-2022-46352	2022-12-13 18:50:49

← Previous ID

Next ID→

© CVE.report 2023 | |
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 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