

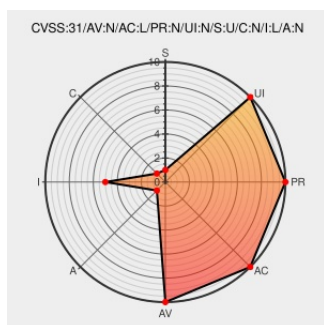


CVE-2022-30229

Published on: Not Yet Published

Last Modified on: 06/23/2022 12:37:00 PM UTC

CVE-2022-30229

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Sicam Gridedge Essential](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SICAM GridEdge Essential ARM (All versions < V2.6.6), SICAM GridEdge Essential Intel (All versions < V2.6.6), SICAM GridEdge Essential with GDS ARM (All versions < V2.6.6), SICAM GridEdge Essential with GDS Intel (All versions < V2.6.6). The affected software does not require authenticated access

for privileged functions. This could allow an unauthenticated attacker to change data of an user, such as credentials, in case that user's id is known.

CVE-2022-30229 has been assigned by [S](#) productcert@siemens.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [S](#) **Siemens - SICAM GridEdge Essential ARM** version **All versions < V2.6.6**

Affected Vendor/Software: [S](#) **Siemens - SICAM GridEdge Essential Intel** version **All versions < V2.6.6**

Affected Vendor/Software: [S](#) **Siemens - SICAM GridEdge Essential with GDS ARM** version **All versions < V2.6.6**

Affected Vendor/Software: [S](#) **Siemens - SICAM GridEdge Essential with GDS Intel** version **All versions < V2.6.6**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	Integrity	Availability

Impact

NONE

Impact

PARTIAL

Impact

NONE

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	 MISC cert-portal.siemens.com/productcert/pdf/ssa-631336.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
Application	Siemens	Sicam Gridedge Essential	All	All	All	All
Application	Siemens	Sicam Gridedge Essential	All	All	All	All
Application	Siemens	Sicam Gridedge Essential	All	All	All	All
Application	Siemens	Sicam Gridedge Essential	All	All	All	All

cpe:2.3:a:siemens:sicam_gridedge_essential:*:*:*:arm:*:*:

cpe:2.3:a:siemens:sicam_gridedge_essential:*:*:*:gds_arm:*:*:

cpe:2.3:a:siemens:sicam_gridedge_essential:*:*:*:gds_intel:*:*:

cpe:2.3:a:siemens:sicam_gridedge_essential:*:*:*:intel:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-30229 : A vulnerability has been identified in SICAM GridEdge Essential ARM All versions < V2.6.6 , SICAM... twitter.com/i/web/status/1...	2022-06-14 09:28:15
 @RedPacketSec	Siemens SICAM GridEdge Software information disclosure CVE-2022-30229 - redpacketsecurity.com/siemens-sicam-...	2022-06-17 09:01:10

← Previous ID

Next ID →

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](#)