



Published on: Not Yet Published

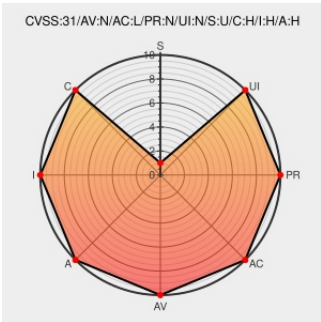
Last Modified on: 05/26/2022 09:02:00 PM UTC

CVE-2022-29873

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [7kg8500-0aa00-0aa0](#) from [Siemens](#) contain the following vulnerability:

[illegible]

P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P850 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00), SICAM P855 (All versions < V3.00). Affected devices do not properly validate parameters of certain GET and POST requests. This could allow an unauthenticated attacker to set the device to a denial of service state or to control the program counter and, thus, execute arbitrary code on the device.

CVE-2022-29873 has been assigned by productcert@siemens.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: 9.8 - CRITICAL

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

UNCHANGED

HIGH

HIGH

HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	 MISC cert-portal.siemens.com/productcert/pdf/ssa-165073.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

590967 Siemens SICAM P850 and SICAM P855 Multiple Vulnerabilities (ICSA-22-132-07) (SSA-165073)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Siemens	7kg8500-0aa00-0aa0	-	All	All	All
Operating System	Siemens	7kg8500-0aa00-0aa0 Firmware	All	All	All	All
Hardware 	Siemens	7kg8500-0aa00-2aa0	-	All	All	All
Operating System	Siemens	7kg8500-0aa00-2aa0 Firmware	All	All	All	All
Hardware 	Siemens	7kg8500-0aa10-0aa0	-	All	All	All
Operating System	Siemens	7kg8500-0aa10-0aa0 Firmware	All	All	All	All
Hardware 	Siemens	7kg8500-0aa10-2aa0	-	All	All	All
Operating System	Siemens	7kg8500-0aa10-2aa0 Firmware	All	All	All	All
Hardware 	Siemens	7kg8500-0aa30-0aa0	-	All	All	All
Operating System	Siemens	7kg8500-0aa30-0aa0 Firmware	All	All	All	All
Hardware 	Siemens	7kg8500-0aa30-2aa0	-	All	All	All
Operating System	Siemens	7kg8500-0aa30-2aa0 Firmware	All	All	All	All

Hardware  	Siemens	7kg8501-0aa01-0aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa01-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa01-2aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa01-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa02-0aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa02-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa02-2aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa02-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa11-0aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa11-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa11-2aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa11-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa12-0aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa12-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa12-2aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa12-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa31-0aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa31-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa31-2aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa31-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa32-0aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa32-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8501-0aa32-2aa0	-	All	All	All
Operating System	Siemens	7kg8501-0aa32-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8550-0aa00-0aa0	-	All	All	All
Operating System	Siemens	7kg8550-0aa00-0aa0 Firmware	All	All	All	All

Hardware  	Siemens	7kg8550-0aa00-2aa0	-	All	All	All
Operating System	Siemens	7kg8550-0aa00-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8550-0aa10-0aa0	-	All	All	All
Operating System	Siemens	7kg8550-0aa10-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8550-0aa10-2aa0	-	All	All	All
Operating System	Siemens	7kg8550-0aa10-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8550-0aa30-0aa0	-	All	All	All
Operating System	Siemens	7kg8550-0aa30-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8550-0aa30-2aa0	-	All	All	All
Operating System	Siemens	7kg8550-0aa30-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa01-0aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa01-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa01-2aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa01-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa02-0aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa02-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa02-2aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa02-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa11-0aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa11-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa11-2aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa11-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa12-0aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa12-0aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa12-2aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa12-2aa0 Firmware	All	All	All	All
Hardware  	Siemens	7kg8551-0aa31-0aa0	-	All	All	All

Operating System	Siemens	7kg8551-0aa31-0aa0 Firmware	All	All	All	All
Hardware	Siemens	7kg8551-0aa31-2aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa31-2aa0 Firmware	All	All	All	All
Hardware	Siemens	7kg8551-0aa32-0aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa32-0aa0 Firmware	All	All	All	All
Hardware	Siemens	7kg8551-0aa32-2aa0	-	All	All	All
Operating System	Siemens	7kg8551-0aa32-2aa0 Firmware	All	All	All	All
cpe:2.3:h:siemens:7kg8500-0aa00-0aa0:-:*****:						
cpe:2.3:o:siemens:7kg8500-0aa00-0aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8500-0aa00-2aa0:-:*****:						
cpe:2.3:o:siemens:7kg8500-0aa00-2aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8500-0aa10-0aa0:-:*****:						
cpe:2.3:o:siemens:7kg8500-0aa10-0aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8500-0aa10-2aa0:-:*****:						
cpe:2.3:o:siemens:7kg8500-0aa10-2aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8500-0aa30-0aa0:-:*****:						
cpe:2.3:o:siemens:7kg8500-0aa30-0aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8500-0aa30-2aa0:-:*****:						
cpe:2.3:o:siemens:7kg8500-0aa30-2aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8501-0aa01-0aa0:-:*****:						
cpe:2.3:o:siemens:7kg8501-0aa01-0aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8501-0aa01-2aa0:-:*****:						
cpe:2.3:o:siemens:7kg8501-0aa01-2aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8501-0aa02-0aa0:-:*****:						
cpe:2.3:o:siemens:7kg8501-0aa02-0aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8501-0aa02-2aa0:-:*****:						
cpe:2.3:o:siemens:7kg8501-0aa02-2aa0_firmware:*****:						
cpe:2.3:h:siemens:7kg8501-0aa11-0aa0:-:*****:						

УРЕ.З.О.И.СИМЕНС./ RY0001-Vaa11-Vaa01.

```
cpe:2.3:o:siemens:7kg8501-0aa11-0aa0_firmware:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:siemens:7kg8501-0aa11-2aa0:-:*:*:*:*:*:*
```

```
cpe:2.3:o:siemens:7kg8501-0aa11-2aa0_firmware:*:*:*:*:*:*:
```

```
cpe:2.3:h:siemens:7kg8501-0aa12-0aa0:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:7kg8501-0aa12-0aa0 firmware:*.***.***.***.
```

```
cpe:2.3:h:siemens:7kq8501-0aa12-2aa0:-:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:7kg8501-0aa12-2aa0_firmware:*.*.*.*.*.*.*.*.*.*
```

cpe:2.3:h:siemens:7kg8501-0aa31-0aa0:-:*:*:*:*:*:

```
cpe:2.3:o:siemens:7kg8501-0aa31-0aa0 firmware:*.***.***.***.
```

```
cpe:2.3:h:siemens:7kg8501-0aa31-2aa0:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:7kg8501-0aa31-2aa0_firmware:*.~*~*~*~*~*~*~*~*~*
```

```
cpe:2.3:h:siemens:7kg8501-0aa32-0aa0:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:7kg8501-0aa32-0aa0_firmware:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:siemens:7kg8501-0aa32-2aa0:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:siemens:7kg8501-0aa32-2aa0_firmware:*.***:*.***:
```

cpe:2.3:h:siemens:7kg8550-0aa00-0aa0:-:*:*:*:*:*:

```
cpe:2.3:o:siemens:7kg8550-0aa00-0aa0_firmware:*.*.*.*.*.*.*.*.*.*
```

cpe:2.3:h:siemens:7kg8550-0aa00-2aa0:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:7kg8550-0aa00-2aa0_firmware:*:*:*:*:*:*:
```

cpe:2.3:h:siemens:7kg8550-0aa10-0aa0:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:7kg8550-0aa10-0aa0_firmware:*.*.*.*.*.*.*.*.*
```

cpe:2.3:h:siemens:7kg8550-0aa10-2aa0:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:7kg8550-0aa10-2aa0_firmware:*:*:*:*:*:*:
```

cpe:2.3:h:siemens:7kg8550-0aa30-0aa0:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:7kg8550-0aa30-0aa0_firmware:*:*:*:*:*:
```

cpe:2.3:h:siemens:7kg8550-0aa30-2aa0:-:*:*:*:*:*:*:

```
cpe:2.3:o:siemens:7kg8550-0aa30-2aa0_firmware:*.*.*.*.*.*.*.*.*.*
```

```
cpe:2.3:h:siemens:7kg8551-0aa01-0aa0:-:*:*:*:*:*:*:
```

cpe:2.3:o:siemens:7kg8551-0aa01-0aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa01-2aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa01-2aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa02-0aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa02-0aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa02-2aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa02-2aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa11-0aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa11-0aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa11-2aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa11-2aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa12-0aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa12-0aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa12-2aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa12-2aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa31-0aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa31-0aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa31-2aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa31-2aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa32-0aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa32-0aa0_firmware:*.*****:
cpe:2.3:h:siemens:7kg8551-0aa32-2aa0:-:*.*****:
cpe:2.3:o:siemens:7kg8551-0aa32-2aa0_firmware:*.*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RedPacketSec	Siemens SICAM P850 and Siemens SICAM P855 denial of service CVE-2022-29873 - redpacketsecurity.com/siemens-sicam-p850-p855-dos-vulnerability/	2022-05-12 09:01:13
 @CVEreport	CVE-2022-29873 : A vulnerability has been identified in SICAM P850 All versions < V3.00 , SICAM P855 All versions < V3.00	2022-05-20 09:01:13

	P850 All versions... twitter.com/i/web/status/1...	13:24:22
 /r/netcve	CVE-2022-29873	2022-05-20 13:39:37
← 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 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](#)