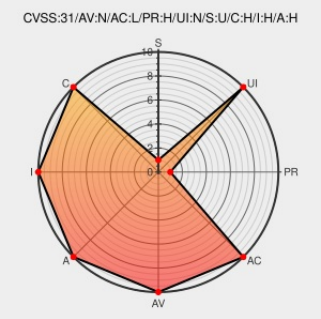
CVE-2020-29000

Published on: 01/25/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-29000

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



Certain versions of Gnc-cw013 from Mygeeni contain the following vulnerability:

An issue was discovered on Geeni GNC-CW013 doorbell 1.8.1 devices. A vulnerability exists in the RTSP service that allows a remote attacker to take full control of the device with a high-privileged account. By sending a crafted message, an attacker is able to remotely deliver a telnet session. Any attacker that has the ability to control DNS can exploit this vulnerability to remotely login to the device and gain access to the camera system.

CVE-2020-29000 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.2 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
My Geeni	Product support.mygeeni.com	MISC support.mygeeni.com/hc/en-us

	text/html	
CVE-2020-29000 · GitHub	Third Party Advisory gist.github.com text/html	MISC gist.github.com/tj-oconnor/d081f5f116a4865f888be81e2466d831

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	Mygeeni	Gnc-cw013	-	All	All	All
Hardware	Mygeeni	Gnc-cw013	-	All	All	All
Operating System	Mygeeni	Gnc-cw013 Firmware	1.8.1	All	All	All
Operating System	Mygeeni	Gnc-cw013 Firmware	1.8.1	All	All	All

cpe:2.3:h:mygeeni:gnc-cw013:-:*:*:*:*:*:*:*:

cpe:2.3:h:mygeeni:gnc-cw013:-:*:*:*:*:*:*:*:

cpe:2.3:o:mygeeni:gnc-cw013_firmware:1.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:mygeeni:gnc-cw013_firmware:1.8.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→