



# CVE-2019-11561

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2019-11561
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-05-08 16:29:00 UTC
<b>Updated</b>	2020-08-24 17:37:00 UTC
<b>Description</b>	The Chuango 433 MHz burglar-alarm product line is vulnerable to a Denial of Service attack. When the condition is triggered

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">Chuango</a>	<a href="#">A11</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">A11</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">A11 Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">A11 Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">A8</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">A8</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">A8 Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">A8 Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">Aww Plus</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">Aww Plus</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">Aww Plus Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">Aww Plus Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">B11</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">B11</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">B11 Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">B11 Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">Cg-105s</a>	-	All	All	All

Hardware	<a href="#">Chuango</a>	<a href="#">Cg-105s</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">Cg-105s Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">Cg-105s Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G3</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G3</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G3 Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G3 Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G5w</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G5w</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G5w 3g</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G5w 3g</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G5w 3g Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G5w 3g Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G5w Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G5w Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G5 Plus</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">G5 Plus</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G5 Plus Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">G5 Plus Firmware</a>	All	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">H4 Plus</a>	-	All	All	All
Hardware	<a href="#">Chuango</a>	<a href="#">H4 Plus</a>	-	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">H4 Plus Firmware</a>	All	All	All	All
Operating System	<a href="#">Chuango</a>	<a href="#">H4 Plus Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
write-ups/CVE-2019-11561 at master · RieeCco/write-ups · GitHub	MISC	<a href="https://github.com">github.com</a>	Third Party Advisory
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)**