



CVE-2019-11061

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-11061
State	PUBLIC
Assigner	cve@cert.org.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-29 01:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	A broken access control vulnerability in HG100 firmware versions up to 4.00.06 allows an attacker in the same local area ne

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Asus	Hg100	-	All	All	All
Hardware	Asus	Hg100	-	All	All	All
Operating System	Asus	Hg100 Firmware	All	All	All	All
Operating System	Asus	Hg100 Firmware	All	All	All	All

References

Reference	Source	Link
TWCERT/CC 台灣電腦網路危機處理暨協調中心	CONFIRM	surl.twc
GitHub - tim124058/ASUS-SmartHome-Exploit: ASUS SmartHome Exploit for CVE-2019-11061 and CVE-2019-11063	CONFIRM	github.c
台灣漏洞紀錄平台 Taiwan Vulnerability Note	CONFIRM	tvn.twce
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

Vendor Comments And Credit

Discovery Credit

LEGACY: timhuang

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

© [CVE.report](#) 2026 |

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](#)