



CVE-2019-11063

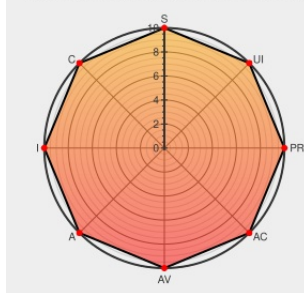
Published on: 08/28/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:36 PM UTC

CVE-2019-11063

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

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



Certain versions of [Smarthome](#) from [Asus](#) contain the following vulnerability:

A broken access control vulnerability in SmartHome app (Android versions up to 3.0.42_190515, ios versions up to 2.0.22) allows an attacker in the same local area network to list user accounts and control IoT devices that connect with its gateway (HG100) via [http://\[target\]/smarthome/devicecontrol](http://[target]/smarthome/devicecontrol) without any authentication.

CVSS 3.0 base score 10 (Confidentiality, Integrity and Availability impacts). CVSS vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

CVE-2019-11063 has been assigned by cve@cert.org.tw to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [ASUS](#) - **SmartHome Android app** version **up to 3.0.42_190515**

Affected Vendor/Software: [ASUS](#) - **SmartHome ios app** version **up to 2.0.22**

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **8.3 - HIGH**

Access Vector	Access Complexity	Authentication
ADJACENT_NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
台灣漏洞紀錄平台 Taiwan Vulnerability Note	Third Party Advisory tvn.twcert.org.tw text/html	CONFIRM tvn.twcert.org.tw/taiwanvn/TVN-201908014
TWCERT/CC 台灣電腦網路危機處理暨協調中心	Third Party Advisory surl.twcert.org.tw text/html Inactive Link Not Archived	CONFIRM surl.twcert.org.tw/5LWQJ
GitHub - tim124058/ASUS-SmartHome-Exploit: ASUS SmartHome Exploit for CVE-2019-11061 and CVE-2019-11063	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/tim124058/ASUS-SmartHome-Exploit/

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

Exploit/POC from Github

ASUS SmartHome Exploit for CVE-2019-11061 and CVE-2019-11063

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Asus	Smarthome	All	All	All	All
Application	Asus	Smarthome	All	All	All	All
Application	Asus	Smarthome	All	All	All	All
Application	Asus	Smarthome	All	All	All	All

cpe:2.3:a:asus:smarthome:*:*:*:*:android:*.*:

cpe:2.3:a:asus:smarthome:*:*:*:*:iphone_os:*.*:

cpe:2.3:a:asus:smarthome:*:*:*:*:android:*.*:

cpe:2.3:a:asus:smarthome:*:*:*:*:iphone_os:*.*:

Discovery Credit

timhuang

[← 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](#)