



CVE-2019-13406

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

Summary

CVE	CVE-2019-13406
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 found in Advan VD-1 firmware versions up to 230. An attacker can send a POST requ

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Androvideo	Vd 1	-	All	All	All
Hardware	Androvideo	Vd 1	-	All	All	All
Operating System	Androvideo	Vd 1 Firmware	All	All	All	All

References

Reference	Source	Link	Tags
AndroVideo Advan VD-1 Multiple Vulnerabilities.md · GitHub	CONFIRM	gist.github.com	Exploit, Third Party Advisory
TWCERT/CC 台灣電腦網路危機處理暨協調中心	CONFIRM	surl.twcert.org.tw	Third Party Advisory
台灣漏洞紀錄平台 Taiwan Vulnerability Note	CONFIRM	tvn.twcert.org.tw	Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

LEGACY: Keniver Wang (CHT Security)

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](#)