



CVE-2022-36381

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

Summary

CVE	CVE-2022-36381
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-16 08:15:00 UTC
Updated	2022-08-17 20:50:00 UTC
Description	OS command injection vulnerability in Nintendo Wi-Fi Network Adaptor WAP-001 All versions allows an attacker with an ad

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nintendo	Wi-fi Network Adaptor Wap 001	-	All	All	All
Operating System	Nintendo	Wi-fi Network Adaptor Wap 001 Firmware	All	All	All	All

References

Reference	Source
JVN#17625382: Multiple vulnerabilities in Nintendo Wi-Fi Network Adaptor WAP-001	MISC
「ニンテンドーWi-Fi USBコネクタ」および「ニンテンドーWi-Fiネットワークアダプタ」使用中止のお願い サポート情報 Nintendo	MISC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report