



CVE-2021-37436

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

Summary

CVE	CVE-2021-37436
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-24 23:15:00 UTC
Updated	2021-08-09 17:26:00 UTC
Description	Amazon Echo Dot devices through 2021-07-02 sometimes allow attackers, who have physical access to a device after a fa

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Amazon	Echo Dot	-	All	All	All
Operating System	Amazon	Echo Dot Firmware	All	All	All	All

References

Reference	Source
dl.acm.org/doi/pdf/10.1145/3448300.3467820	MISC
Amazon Echo Dot Does Not Wipe Personal Content After Factory Reset Hacker News	MISC
Is It Possible To Make IoT Devices Private? Amazon Echo Dot Does Not Wipe Personal Content After Factory Reset - CPO Magazine	MISC
Thinking about selling your Echo Dot—or any IoT device? Read this first Ars Technica	MISC
CVE Program record	CVE
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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](#)