



CVE-2020-11723

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

Summary

CVE	CVE-2020-11723
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-14 20:15:00 UTC
Updated	2020-04-22 16:59:00 UTC
Description	Cellebrite UFED 5.0 through 7.29 uses four hardcoded RSA private keys to authenticate to the ADB daemon on target device

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cellebrite	Ufed	-	All	All	All
Hardware	Cellebrite	Ufed	-	All	All	All
Operating System	Cellebrite	Ufed Firmware	All	All	All	All

References

Reference	Source	Link
Cellebrite UFED 7.29 Hardcoded ADB Authentication Keys ≈ Packet Storm	MISC	packets
UFED and Cellebrite Responder 7.30 provides new support for smartphones with Huawei KIRIN processor - Cellebrite	MISC	www.ce
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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

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](#).

Free CVE JSON API cve.report/api

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