



CVE-2019-18672

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

Summary

CVE	CVE-2019-18672
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-06 18:15:00 UTC
Updated	2020-03-02 15:15:00 UTC
Description	Insufficient checks in the finite state machine of the ShapeShift KeepKey hardware wallet before firmware 6.2.2 allow a part

Risk And Classification

Problem Types: CWE-354

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Shapeshift	Keepkey Firmware	-	All	All	All
Hardware	Shapeshift	Keepkey Firmware	-	All	All	All
Operating System	Shapeshift	Keepkey Firmware	All	All	All	All
Operating System	Shapeshift	Keepkey Firmware	All	All	All	All

References

Reference	Source	L
KeepKey Release Notes — v6.2.2. Download the latest KeepKey Client and... by ShapeShift ShapeShift Stories Medium	MISC	r
firmware: stronger recovery state machine checks · keepkey/keepkey-firmware@769714f · GitHub	MISC	g
ShapeShift Security Update - ShapeShift Stories - Medium	CONFIRM	r
KeepKey key erasure vulnerability (VULN-1971) invd blog	MISC	b
CVE Program record	CVE.ORG	v
NVD vulnerability detail	NVD	r

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)