



CVE-2017-17877

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2017-17877
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-27 17:08:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An issue was discovered in Valve Steam Link build 643. When the SSH daemon is enabled for local development, the device

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Valvesoftware	Steam Link	-	All	All	All
Hardware	Valvesoftware	Steam Link	-	All	All	All
Operating System	Valvesoftware	Steam Link Firmware	All	All	All	All
Operating System	Valvesoftware	Steam Link Firmware	All	All	All	All

References

Reference	Source	Link	T
GitHub - ValveSoftware/steamlink-sdk: An SDK for creating native Steam Link applications	MISC	github.com	ks
RFC 3514: Steam Link Security - Remotely Insecure SSH - Part #2	MISC	blogger.davidmanouchehri.com	ks
github.com/ValveSoftware/steamlink-sdk/issues/119	MISC	github.com	ks
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

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](#)