



CVE-2016-5119

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

Summary

CVE	CVE-2016-5119
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-23 21:59:00 UTC
Updated	2017-01-24 21:18:00 UTC
Description	The automatic update feature in KeePass 2.33 and earlier allows man-in-the-middle attackers to execute arbitrary code by :

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Keepass	Keepass	All	All	All	All

References

Reference	Source	Link
KeepPass 2 Man-In-The-Middle ~ Packet Storm	MISC	packetstormsecurity.com
KeepPass / Discussion / Open Discussion: CVE-2016-5119: MitM Attack against KeePass 2's Update Check	CONFIRM	sourceforge.net
CVE-2016-5119: MitM Attack against KeePass 2's Update Check » bogner.sh	MISC	bogner.sh
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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