



CVE-2022-0725

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

Summary

CVE	CVE-2022-0725
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-03-10 17:44:00 UTC
Updated	2022-10-28 18:14:00 UTC
Description	A flaw was found in keepass. The vulnerability occurs due to logging the plain text passwords in system log and leads to an

Risk And Classification

Problem Types: CWE-532

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	Extra Packages For Enterprise Linux	7.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Fedoraproject	Fedora Extra Packages For Enterprise Linux	7.0	All	All	All
Application	Keepass	Keepass	2.48	All	All	All

References

Reference	Source	Li
GitHub - ByteHackr/keepass_poc: POC for KeePass [CVE-2022-0725]	MISC	git
2052696 – (CVE-2022-0725) CVE-2022-0725 keepass: logs plain text passwords in system log when clearing the clipboard	MISC	bu
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

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](#)