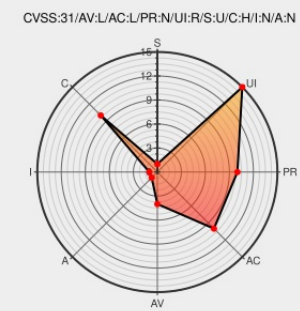
CVE-2023-24055

Published on: Not Yet Published

Last Modified on: 02/02/2023 12:15:00 AM UTC

CVE-2023-24055

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Keepass from Keepass contain the following vulnerability:

** DISPUTED ** KeePass through 2.53 (in a default installation) allows an attacker, who has write access to the XML configuration file, to obtain the cleartext passwords by adding an export trigger. NOTE: the vendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC.

CVE-2023-24055 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVE References

Description	Tags	Link
Just a moment...	sourceforge.net, text/html, Inactive Link, Not Archived	MISC sourceforge.net/p/keepass/discussion/329220/thread/a146e5cf6b/
Another Password Manager Leak Bug: But KeePass Denies CVE - Security Boulevard	securityboulevard.com, text/html	MISC securityboulevard.com/2023/01/keepass-password-manager-leak-cve-richixbw/
Just a moment...	sourceforge.net, text/html, Inactive Link, Not Archived	MISC sourceforge.net/p/keepass/feature-requests/2773/

comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2023-24055 PoC (KeePass 2.5x)

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:keepass:keepass:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-24055 : ** DISPUTED ** KeePass through 2.53 in a default installation allows an attacker, who has write… twitter.com/i/web/status/1…	2023-01-22 04:07:18
@InteraxisCA	NVD - CVE-2023-24055: KeePass through 2.53 (in a default installation) allows an attacker, who has write access to… twitter.com/i/web/status/1…	2023-01-22 11:45:32
@threatmeter	CVE-2023-24055 | KeePass up to 2.53 XML Configuration File missing encryption A vulnerability was found in KeePass… twitter.com/i/web/status/1…	2023-01-22 11:50:35
/r/KeePass	CVE-2023-24055: Keepass vulnerability	2023-01-26 14:15:29
/r/apdm	CVE-2023-24055 : KeePass affecté par une faille critique !	2023-01-27 01:11:27
/r/blueteamsec	CVE-2023-24055 PoC (KeePass 2.5x) - An attacker who has write access to the KeePass configuration file can modify it and inject malicious triggers, e.g to obtain the cleartext passwords by adding an export trigger	2023-01-28 19:43:44
/r/SecOpsDaily	GitHub - alt3kx/CVE-2023-24055_PoC: CVE-2023-24055 PoC (KeePass 2.5x)	2023-01-30 14:12:40
/r/france	CVE-2023-24055 : KeePass affecté par une faille critique !	2023-01-30 14:11:14
/r/discussion_patiente	CVE-2023-24055 : KeePass affecté par une faille critique !	2023-01-30 18:46:31
/r/cybersecurity	KeePass disputes vulnerability allowing stealthy password theft even as countries issue advisories regarding CVE-2023-24055	2023-01-31 15:18:10
/r/u/Great-Campaign7709	KeePass disputes vulnerability allowing stealthy password theft even as countries issue advisories regarding CVE-2023-24055	2023-01-31 21:43:38
/r/KibernetinisSaugumas	"KeePass" nepriima naudotojų skundų dėl pažeidžiamumų savo sistemose	2023-02-02 11:37:07
/r/KeePass	KeePass CVE-2023-24055 PoC and KeePassDX and KeePassXC question	2023-02-03 04:04:54

04:04:54

← Previous ID

Next ID→