



CVE-2023-38840

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

Summary

CVE	CVE-2023-38840
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-08-15 17:15:00 UTC
Updated	2023-08-22 14:58:00 UTC
Description	Bitwarden Desktop 2023.7.0 and below allows an attacker with local access to obtain sensitive information via the Bitwarden Desktop application.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
Erase Master Password in memory after login · Issue #476 · bitwarden/desktop · GitHub	MISC	git
GitHub - markuta/bw-dump: A proof-of-concept that extracts plaintext master passwords from a locked Bitwarden vault.	MISC	git
Hunting for Bitwarden master passwords stored in memory Red Maple Technologies	MISC	rec
[PM-1898] Change desktop reload to `forcefullyCrashRenderer` by Hinton · Pull Request #5813 · bitwarden/clients · GitHub	MISC	git
CVE Program record	CVE.ORG	vw
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.

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](#)