



CVE-2021-36750

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

Summary

CVE	CVE-2021-36750
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-22 14:15:00 UTC
Updated	2022-01-06 14:13:00 UTC
Description	ENC DataVault before 7.2 and VaultAPI v67 mishandle key derivation, making it easier for attackers to determine the passw

Risk And Classification

Problem Types: CWE-307

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sandisk	Secureaccess	3.02	All	All	All
Application	Zendesk	Enc Datavault	All	All	All	All
Application	Zendesk	Enc Vaultapi	All	All	All	All

References

Reference	Source	Link	Tags
Practical bruteforce of military grade AES-1024 :: Remote Rhein Ruhr Stage :: pretalx	MISC	pretalx.c3voc.de	
Update for ENC Software – ENC Security Help Center	MISC	encsecurity.zendesk.com	
WDC-21014 SanDisk SecureAccess Software Update Western Digital	MISC	www.westerndigital.com	
ENCSecurity	MISC	www.encsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[376264](#) ENC DataVault Mishandle Key Derivation Vulnerability

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)