



CVE-2021-43008

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

Summary

CVE	CVE-2021-43008
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-04-05 02:15:00 UTC
Updated	2022-09-30 13:03:00 UTC
Description	Improper Access Control in Adminer versions 1.12.0 to 4.6.2 (fixed in version 4.6.3) allows an attacker to achieve Arbitrary

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adminer	Adminer	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

References

Reference	Source	Link	Tags
PHP tool 'Adminer' leaks passwords – Sansec	MISC	sansec.io	
Adminer - Database management in a single PHP file	MISC	www.adminer.org	
Release v4.6.3 · vrana/adminer · GitHub	MISC	github.com	
[SECURITY] [DLA 3002-1] adminer security update	MLIST	lists.debian.org	
CVE-2021-43008 - Adminer - Arbitrary file read · Podalirius	MISC	podalirius.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179285](#) Debian Security Update for adminer (DLA 3002-1)

© [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](#)