

CVE-2021-21311

Adminer Server-Side Request Forgery Vulnerability

CISA KEV since Sep 29, 2025

Actively exploited

Adminer is an open-source database management in a single PHP file. In adminer from version 4.0.0 and before 4.7.9 there is a server-side request forgery vulnerability. Users of Adminer versions bundling all drivers (e.g. `adminer.php`) are affected. This is fixed in version 4.7.9.

EVRS 84 /100 Urgent priority	CVSS V3.1 7.2 High · NVD	EPSS 0.985 99.92nd percentile · FIRST	CISA DEADLINE Oct 20, 2025 KEV since 2025 · listed over a year
---	--	---	--

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	Added to CISA KEV within the last two years
☒ EPSS	0.985 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.2	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
vrana/adminer	< 4.7.9	4.7.9	GitHub
adminer	≥ 4.0.0 < 4.7.9	no fixed version listed	NVD
debian linux	9.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/vrana/adminer/commit/ccd2374b0b12bd547417bf0dacdf153826c83351	github.com	github.com/vrana/adminer/security/advisories/GHSA-x5r2-hj5c-8jx6
NVD	nvd.nist.gov/vuln/detail/CVE-2021-21311	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
GitHub advisory	github.com/advisories/GHSA-x5r2-hj5c-8jx6	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-0576
Current data	evulnable.com/vulnerability-management/cve/CVE-2021-21311		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.