aDvens

Security for the greater good

Newscast

Critical vulnerability in Apache

2024-01-09 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

Table of content

CVE-2023-27524

Initially discoverd on 11 October 2021, this critical *Insecure Default Initialisation of Resource* vulnerability was the subject of an alert by *Apache* on 24 April 2023.

The lack of rules forcing users to change default passwords (*SECRET_KEY*) allows a remote unauthenticated attacker, by sending a specially crafted request, to bypass access policies and obtain sensitive information.

Update from 09 January 2024 :CISA added this vulnerability to its *Known Exploited Vulnerabilities (KEV)* database on 8 January 2024.

Type of vulnerability

- **CWE-284**: Improper Access Control

Risks

- Security policy bypass
- Impact on Confidentiality
- Impact on Integrity

Criticality (CVSS v3.1 base score)

Attack vector	Network	Scope	Unchanged
Attack complexity	Low	Impact on confidentiality	High
Privileges Required	None	Impact on integrity	High
User Interaction	None	Impact on availability	High

Products impacted

- Apache Superset versions 2.0.1 et earlier

Recommendations

- Update Apache Superset to the version 2.1.0 or later.
- Additional information is available in Apache's advisory.

Proof of concept

A proof of concept is available in open source.

Sources

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-27524
- https://lists.apache.org/thread/n0ftx60sllf527j7g11kmt24wvof8xyk
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2024/01/08/cisa-adds-six-known-exploited-vulnerabilities-catalog