

BLOG

TRIAL ENQUIRY

SUPPORT PORTAL

中文

PORTUGUESE



CLOUD-DELIVERED SERVICES ▼

PRODUCTS ▼

SOLUTIONS ▼

SUPPORT & SERVICES ▼

RESOURCES ▼

NEWS AND EVENTS ▼

COMPANY ▼

UNDER ATTACK? CALL US

# APACHE SOLR ARBITRARY FILE READ AND SSRF VULNERABILITY THREAT ALERT

## Apache Solr Arbitrary File Read and SSRF Vulnerability Threat Alert

March 29, 2021 | Jie Ji



CLOUD-DELIVERED SERVICES ▼

PRODUCTS ▼

SOLUTIONS ▼

SUPPORT & SERVICES ▼

RESOURCES ▼

NEWS AND EVENTS ▼

COMPANY ▼

UNDER ATTACK? CALL US

## Vulnerability Description

Recently, NSFOCUS detected that an Apache Solr arbitrary file read and server-side request forgery (SSRF) vulnerability was disclosed on the Internet. Since authentication was disabled by default when Apache Solr was installed, unauthenticated attackers could turn on requestDispatcher.requestParsers.enableRemoteStreaming via the Config API, thereby exploiting the vulnerability to read files. Currently, the proof of concept (PoC) of this vulnerability has been made publicly available. Relevant users are advised to take protective measures as soon as possible.

Apache Solr is an open-source enterprise search platform from the Apache Lucene project. It is written in Java and runs as a standalone full-text search server within a servlet container such as Apache Tomcat or Jetty. Its major features include powerful full-text search, hit highlighting, faceted search, dynamic clustering, database integration, and rich document handling.

Reference link: <https://issues.apache.org/jira/browse/SOLR?spm=a2c4g.11174386.n2.4.4fda1051uA9TBw>

## Scope of Impact

### Affected Versions

- Apache Solr <= 8.8.1 (all versions)

## Mitigation

The vendor has not fixed the vulnerability, so secure versions are unavailable.

### Protection Measures



CLOUD-DELIVERED SERVICES ▼

PRODUCTS ▼

SOLUTIONS ▼

SUPPORT & SERVICES ▼

RESOURCES ▼

NEWS AND EVENTS ▼

COMPANY ▼

UNDER ATTACK? CALL US

and/or using this advisory. NSFOCUS reserves all the rights to modify and interpret this advisory. Please include this statement paragraph when reproducing or transferring this advisory. Do not modify this advisory, add/delete any information to/from it, or use this advisory for commercial purposes without permission from NSFOCUS.



## CLOUD- DELIVERED SERVICES

Cloud DDoS  
Protection  
Service

Continuous  
Threat Exposure  
Management

Threat  
Intelligence  
Service



- CLOUD-DELIVERED SERVICES ▼
- PRODUCTS ▼
- SOLUTIONS ▼
- SUPPORT & SERVICES ▼
- RESOURCES ▼
- NEWS AND EVENTS ▼
- COMPANY ▼

UNDER ATTACK? CALL US

- Next-Generation Firewall
- Next Generation Intrusion Prevention
- Security Assessment Services
- NSFOCUS Managed Security Services
- Training Services
- Management Team
- NSFOCUS Security Labs
- Careers
- Contact Us

