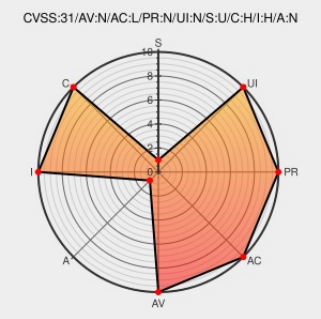
CVE-2021-26715

Published on: 03/25/2021 12:00:00 AM UTC

Last Modified on: 03/29/2021 07:03:00 PM UTC

CVE-2021-26715

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Connect from Mitreid contain the following vulnerability:

The OpenID Connect server implementation for MITREid Connect through 1.3.3 contains a Server Side Request Forgery (SSRF) vulnerability. The vulnerability arises due to unsafe usage of the logo_uri parameter in the Dynamic Client Registration request. An unauthenticated attacker can make a HTTP request from the vulnerable server to any address in the internal network and obtain its response (which might, for example, have a JavaScript payload for resultant XSS). The issue can be exploited to bypass network boundaries, obtain sensitive data, or attack other hosts in the internal network.

CVE-2021-26715 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Releases · mitreid-connect/OpenID-Connect-Java-Spring-Server · GitHub	github.com text/html	MISC github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server/releases
Hidden OAuth attack vectors | PortSwigger Research	portswigger.net text/html	MISC portswigger.net/research/hidden-oauth-attack-vectors

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

982593 Java (maven) Security Update for org.mitre:openid-connect-server (GHSA-792r-mh2q-p8qp)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mitreid	Connect	All	All	All	All

cpe:2.3:a:mitreid:connect:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@elhackernet	Vectores de ataque #OAuth ocultos - Server Side Request Forgery #SSRF CVE-2021-26715 #OpenID… twitter.com/i/web/status/1…	2021-04-01 09:35:00

← Previous ID

Next ID→