

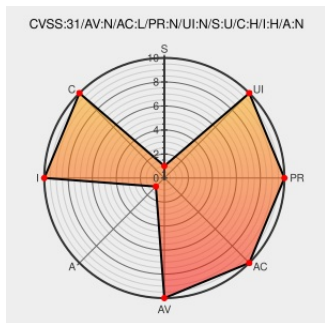


CVE-2021-27582

Published on: 02/23/2021 12:00:00 AM UTC

Last Modified on: 12/02/2022 07:37:00 PM UTC

CVE-2021-27582

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Connect](#) from [Mitreid](#) contain the following vulnerability:

[org/mitre/oauth2/web/OAuthConfirmationController.java](#) in the OpenID Connect server implementation for MITREid Connect through 1.3.3 contains a Mass Assignment (aka Autobinding) vulnerability. This arises due to unsafe usage of the `@ModelAttribute` annotation during the OAuth authorization flow, in which HTTP request parameters affect an `authorizationRequest`.

CVE-2021-27582 has been assigned by [M](#) [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
GreenDog's blog: Autobinding vulns and Spring MVC	Exploit Third Party Advisory	MISC agrrrdog.blogspot.com/2017/03/autobinding-vulns-and-spring-mvc.html

agrrrdog.blogspot.com
text/html

Fix Spring Autobinding vulnerability · mitreid-connect/OpenID-Connect-Java-Spring-Server@7eba3c1 · GitHub

Patch
Third Party Advisory
github.com
text/html

MISC github.com/mitreid-connect/OpenID-Connect-Java-Spring-Server/commit/7eba3c12fed82388f917e8dd9b73e86e3a311e4c

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

982592 Java (maven) Security Update for org.mitre:openid-connect-parent (GHSA-8p36-q63g-68qh)

Exploit/POC from Github

org/mitre/oauth2/web/OAuthConfirmationController.java in the OpenID Connect server implementation for MITREid Connect...

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)
 @RemotelyAlerts	Severity: ?? org/mitre/oauth2/web/OAuthConfirmationCo... CVE-2021-27582 Link for more: alerts.remotelyrmm.com/CVE-2021-27582	2022-04-26 15:32:21

← Previous ID

Next ID →

© CVE.report 2023   |

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve/).

CVE.report and Source URL Uptime Status status.cve.report