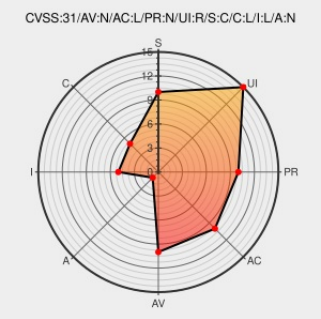
CVE-2020-5497

Published on: 01/03/2020 12:00:00 AM UTC

Last Modified on: 01/24/2023 01:59:00 AM UTC

CVE-2020-5497

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



Certain versions of Connect from Mitreid contain the following vulnerability:

The OpenID Connect reference implementation for MITREid Connect through 1.3.3 allows XSS due to userInfoJson being included in the page unsanitized. This is related to header.tag. The issue can be exploited to execute arbitrary JavaScript.

CVE-2020-5497 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
MITREid 1.3.3 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/156574/MITREid-1.3.3-Cross-Site-Scripting.html
Cross-Site Scripting header.tag · Issue #1521 · mitreid-	Exploit	MISC github.com/mitreid-connect/OpenID-

connect/OpenID-Connect-Java-Spring-Server · GitHub	Issue Tracking Third Party Advisory github.com text/html	Connect-Java-Spring-Server/issues/1521
CVE-2020-5497 - MITREid Connect Cross-site Scripting	www.securitymetrics.com text/html	SM MISC www.securitymetrics.com/blog/MITREid-Connect-cross-site-scripting-CVE-2020-5497
Full Disclosure: CVE-2020-5497 - MITREid Connect XSS	seclists.org text/html	FULLDISC 20200227 CVE-2020-5497 - MITREid Connect XSS

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

981568 Java (maven) Security Update for org.mitre:openid-connect-server (GHSA-c2h6-7gm8-cv4w)

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

← Previous ID

Next ID→