



CVE-2021-20786

Published on: 07/27/2021 12:00:00 AM UTC

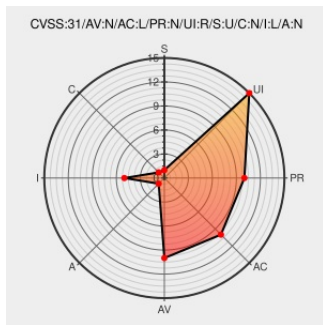
Last Modified on: 08/06/2021 07:32:00 PM UTC

CVE-2021-20786

Source: Mitre

Source: Nist

Print: PDF



Certain versions of **Groupsession** from **Groupsession** contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in GroupSession (GroupSession Free edition from ver2.2.0 to the version prior to ver5.1.0, GroupSession byCloud from ver3.0.3 to the version prior to ver5.1.0, and GroupSession ZION from ver3.0.3 to the version prior to ver5.1.0) allows a remote attacker to hijack the authentication of administrators via a specially crafted URL.

CVE-2021-20786 has been assigned by vultures@jpcert.or.jp to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: Japan Total System Co.,Ltd. - **GroupSession** version **GroupSession Free edition from ver2.2.0 to the version prior to ver5.1.0, GroupSession byCloud from ver3.0.3 to the version prior to ver5.1.0, and GroupSession ZION from ver3.0.3 to the version prior to ver5.1.0**

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	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
JVN#86026700: Multiple vulnerabilities in GroupSession	jvn.jp text/xml	MISC jvn.jp/en/jp/JVN86026700/index.html
GroupSessionは組織を強化するグループウェア 無料版、エンタープライズ版、クラウド型をラインナップ！	groupsession.jp text/html	MISC groupsession.jp/info/info-news/security202107
<p>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.</p>		

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC for exploiting CVE-2021-20786 : Cross-site request forgery (CSRF) vulnerability in GroupSession (GroupSession Fre...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Groupsession	Groupsession	All	All	All	All
Application	Groupsession	Groupsession Bycloud	All	All	All	All
Application	Groupsession	Groupsession Zion	All	All	All	All
cpe:2.3:a:groupsession:groupsession:*:*:*:free:*:*:						
cpe:2.3:a:groupsession:groupsession_bycloud:*:*:*:*:*:						
cpe:2.3:a:groupsession:groupsession_zion:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-20786 : Cross-site request forgery CSRF vulnerability in GroupSession GroupSession Free edition from ve... twitter.com/i/web/status/1...	2021-07-28 00:52:19

[← Previous ID](#)

[Next ID →](#)

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)