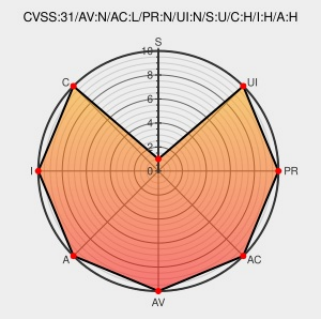
CVE-2021-25981

Published on: 01/03/2022 12:00:00 AM UTC

Last Modified on: 01/14/2022 06:26:00 PM UTC

CVE-2021-25981 - advisory for https://www.whitesourcesoftware.com/vulnerability-database/

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



Certain versions of Talkyard from Talkyard contain the following vulnerability:

In Talkyard, regular versions v0.2021.20 through v0.2021.33 and dev versions v0.2021.20 through v0.2021.34, are vulnerable to Insufficient Session Expiration. This may allow an attacker to reuse the admin's still-valid session token even when logged-out, to gain admin privileges, given the attacker is able to obtain that token (via other, hypothetical attacks)

CVE-2021-25981 has been assigned by vulnerabilitylab@whitesourcesoftware.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **debiki** - **talkyard** version **>= v0.2021.20**

Affected Vendor/Software: **debiki** - **talkyard** version **<= v0.2021.34**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
Better session ids, 5 parts, feature flag to enable. · debiki/talkyard@b0310df · GitHub	github.com text/html	MISC github.com/debiki/talkyard/commit/b0310df019887f3464895529c773bc7d85ddcf34
Use fancy sids, not silly sids, by default. · debiki/talkyard@b071291 · GitHub	github.com text/html	MISC github.com/debiki/talkyard/commit/b0712915d8a22a20b09a129924e8a29c25ae57
CVE-2021-25981 | WhiteSource Vulnerability Database	www.whitesourcesoftware.com text/html	MISC www.whitesourcesoftware.com/vulnerability-database/CVE-2021-25981

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Talkyard	Talkyard	All	All	All	All

cpe:2.3:a:talkyard:talkyard:*:*:*:*:*:*:*:*:

Discovery Credit

WhiteSource Vulnerability Research Team (WVR)

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-25981 : In Talkyard, regular versions v0.2021.20 through v0.2021.33 and dev versions v0.2021.20 through v0… twitter.com/i/web/status/1…	2022-01-03 06:38:17
@SecRiskRptSME	RT: CVE-2021-25981 In Talkyard, regular versions v0.2021.20 through v0.2021.33 and dev versions v0.2021.20 through… twitter.com/i/web/status/1…	2022-01-03 08:33:34

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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