



CVE-2021-29437

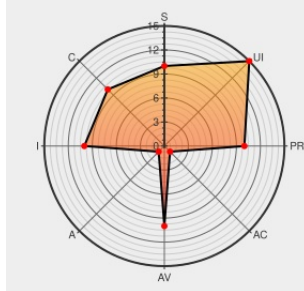
Published on: 04/13/2021 12:00:00 AM UTC

Last Modified on: 06/26/2023 07:10:00 PM UTC

CVE-2021-29437 - advisory for GHSA-gvpg-23fh-8g75

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

CVSS:31/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N



Certain versions of [Scratchoauth2](#) from [Scratchoauth2 Project](#) contain the following vulnerability:

ScratchOAuth2 is an OAuth implementation for Scratch. Any ScratchOAuth2-related data normally accessible and modifiable by a user can be read and modified by a third party. 1. Scratch user visits 3rd party site. 2. 3rd party site asks user for Scratch username. 3. 3rd party site pretends to be user and gets login code from ScratchOAuth2. 4. 3rd party site gives code to user and instructs them to post it on their profile. 5. User posts code on their profile, not knowing it is a ScratchOAuth2 login code. 6. 3rd party site completes login with ScratchOAuth2. 7. 3rd party site has full access to anything the user could do if they directly logged in. See referenced GitHub security advisory for patch notes and workarounds.

CVE-2021-29437 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **ScratchVerifier** - **ScratchOAuth2** version < 9220c2a

CVSS3 Score: **6.8 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
SECURITY: Mitigate MITM (GHSA-gvpg-23fh-8g75) · ScratchVerifier/ScratchOAuth2@9220c2a · GitHub	github.com text/html	MISC github.com/ScratchVerifier/ScratchOAuth2/commit/9220c2a77eda3df37a84486ad7
Account compromise by man-in-the-middle attack · Advisory · ScratchVerifier/ScratchOAuth2 · GitHub	github.com text/html	CONFIRM github.com/ScratchVerifier/ScratchOAuth2/security/advisories/GHSA-

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Scratchoauth2 Project	Scratchoauth2	All	All	All	All

cpe:2.3:a:scratchoauth2_project:scratchoauth2:*:*:*:*:scratch:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-29437 : ScratchOAuth2 is an Oauth implementation for Scratch. Any ScratchOAuth2-related data normally acce... twitter.com/i/web/status/1...	2021-04-13 20:22:46
/r/netcve	CVE-2021-29437	2021-04-13 20:25:00

← Previous ID

Next ID →