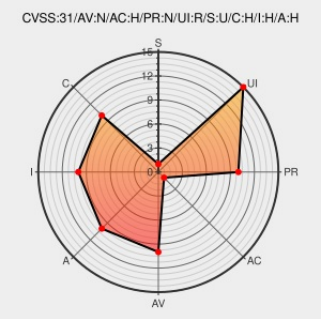
CVE-2020-26236

Published on: 11/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:55 PM UTC

CVE-2020-26236 - advisory for GHSA-99cr-hvf7-85g9

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



Certain versions of Scratchverifier from Scratchverifier contain the following vulnerability:

In ScratchVerifier before commit a603769, an attacker can hijack the verification process to log into someone else's account on any site that uses ScratchVerifier for logins. A possible exploitation would follow these steps: 1. User starts login process. 2. Attacker attempts login for user, and is given the same verification code. 3. User comments code as part of their normal login. 4. Before user can, attacker completes the login process now that the code is commented. 5. User gets a failed login and attacker now has control of the account. Since commit a603769 starting a login twice will generate different verification codes, causing both user and attacker login to fail. For clients that rely on a clone of ScratchVerifier not hosted by the developers, their users may attempt to finish the login process as soon as possible after commenting the code. There is no reliable way for the attacker to know before the user can finish the process that the user has commented the code, so this vulnerability only really affects those who comment the code and then take several seconds before finishing the login.

CVE-2020-26236 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **ScratchVerifier** - **ScratchVerifier** version **< a603769**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5.1 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	HIGH	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Change behavior of PUT /verify/{} · ScratchVerifier/ScratchVerifier@a603769 · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/ScratchVerifier/ScratchVerifier/commit/a603769010abf8c1bede9
Verification Code Hijacking · Advisory · ScratchVerifier/ScratchVerifier · GitHub	Third Party Advisory, github.com, text/html	CONFIRM github.com/ScratchVerifier/ScratchVerifier/security/advisories/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

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

cpe:2.3:a:scratchverifier:scratchverifier:*:*:*:*:*:*:*:*:

cpe:2.3:a:scratchverifier:scratchverifier:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→