Published: Aug 18, 2021 Version: 1.0

# FSA-2021-1 Missing User Presence Check in webauthn-framework

## 1 Vulnerability

| | |
|---|---|
| **FZI-ID** | FZI-2021-4 |
| **CVE** | CVE-2021-38299 |
| **Manufacturer** | Spomky Labs |
| **Product** | webauthn-framework |
| **Affected Version** | < 3.2.9, 3.3.0-3.3.3 |
| **Type** | CWE-287 - Improper Authentication - Generic |
| **Date Found** | 13.04.2021 |
| **Discovered By** | Timon Hackenjos |
| **Patch Available** | Yes |
| **Patch Version** | 3.3.4 |
| **CVSS Score** | 5.9 (Medium) |
| **CVSS String** | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L |

The PHP library webauthn-framework did not verify the user present bit of WebAuthn assertions. Thus, an attacker with remote access to a user's system might use an attached authenticator to login to a vulnerable service without physically pressing a button or passing a test of user presence by other means.

WebAuthn enables the use of public-key authentication in the web and is part of the FIDO2 standard. According to the standard, authenticators can be requested to generate assertions without requiring a test of user presence, however they must set the user present bit in an assertion accordingly. This bit is part of the signed data and can thus not be manipulated outside of the authenticator. Even though Web browsers always request a check of user presence, an attacker with direct access to an authenticator might request an assertion without a user presence check. Thus, the relying party is required to verify that the user present bit is set in an assertion.

Note that this is not a critical issue and users and developers are still encouraged to use FIDO2 instead of passwords. Nonetheless, applications should update the library to further increase security.

## 2 Mitigation

The behavior is fixed in version 3.3.4.

# 3 Disclosure Timeline

- 13.04.2021: Reported finding to developer of webauthn-framework
- 16.04.2021: Developer releases fixed version 3.3.4
- 20.04.2021: Developer requests CVE-ID
- 20.04.2021: Asked if the developer puts out a security note
- 20.04.2021: Developer confirms that he adds a security note
- 22.04.2021: Developer reports CVE-ID
- 22.04.2021: Asked the developer when the security note will be published
- 27.04.2021: Asked for an update
- 04.05.2021: Asked why 2.1.5 is still marked as latest release
- 28.05.2021: Asked for another update
- 03.08.2021: Asked for an update regarding the CVE
- 09.08.2021: Request for CVE-ID from MITRE
- 09.08.2021: MITRE assigns CVE-2021-38299
- 18.08.2021: Publication