heise Security

YubiKey: Yubico ruft Security-Keys der FIPS-Serie zurück

Alert! 18.06.2019 12:41 Uhr
Olivia von Westernhagen

(Bild: Yubico)

Besitzer einiger YubiKeys der FIPS-Serie erhalten kostenlosen Ersatz – denn in zwei Firmware-Versionen klafft eine schwere Sicherheitslücke.

Zwei Firmware-Versionen der FIPS-Serie des Security-Tokens YubiKey weisen einen Programmierfehler auf. Er reduziert die Zufälligkeit von Werten, die die betroffenen Tokens während der Startphase generieren.

Die FIPS-Serie ist jene, die laut Webseite des Herstellers Yubico "dem höchsten Sicherheitsstandard für Authentikatoren (AAL3) sowie der neuen NIST SP800-63B Richtlinie" entspricht. Die Federal Information Processing Standards (FIPS) werden von der US-Regierung festgelegt. Produkte, die ihnen entsprechen, werden häufig im Regierungsumfeld oder auch beim Militär eingesetzt.

In einem Sicherheitshinweis schreibt Yubico, dass die reduzierte Zufälligkeit "die allerersten kryptografischen Operationen" nach Aktivierung des Security-Keys betreffe [1]. In einigen Fällen lässt sich die Authentifizierungssicherheit komplett aushebeln. Vor allem mit einem verwundbaren Key erstellte ECDSA-Signaturen werden laut Sicherheitshinweis stark geschwächt: Angreifer, die in den Besitz mehrerer solcher

Signaturen kämen, könnten daraus unter Umständen den privaten Schlüssel rekonstruieren. Die Generierung von RSA-Keys würde durch den Fehler hingegen nicht ausreichend beeinträchtigt, um Daten zu entschlüsseln oder gar an den privaten Key zu gelangen.

Kostenlose Rückgabe möglich

Yubico hat ein Replacement Portal eingerichtet [2], über das Besitzer eines verwundbaren Keys kostenlosen Ersatz anfordern können. Vom Programmierfehler betroffen sind die Modelle **YubiKey FIPS, YubiKey Nano FIPS, YubiKey C FIPS und YubiKey C Nano FIPS**, sofern auf ihnen die **Firmware 4.4.2 oder 4.4.4** installiert ist. Auf den "Ersatzschlüsseln" läuft die Ende April erschienene, abgesicherte Version 4.4.5. (**ovw [3]**)

URL dieses Artikels:
`http://www.heise.de/-4448794`

Links in diesem Artikel:
[1] `https://www.yubico.com/support/security-advisories/ysa-2019-02/`
[2] `https://www.yubico.com/replaceorder/`
[3] `mailto:ovw@heise.de`