2020-04

Security Advisory YSA-2020-04 – Access code not checked for NDEF updates

Published date: 2020-07-08
Tracking ID: YSA-2020-04
CVE: CVE-2020-15001

Summary

The OTP application on the YubiKey 5 NFC allows a user to set optional access codes on OTP slots. This access code is intended to prevent unauthorized changes to OTP configurations. It was discovered that the access code is not checked when updating NFC-specific components of the OTP configurations. This may allow an attacker to access configured OTPs and passwords stored in slots that were not configured by the user to be read over NFC, despite a user having set an access code. Users who have not set an access code, or who have not configured the OTP slots, are not impacted by this issue.

Affected devices

YubiKey 5 NFC with firmware versions 5.0.0 to 5.2.6 and 5.3.0 to 5.3.1.

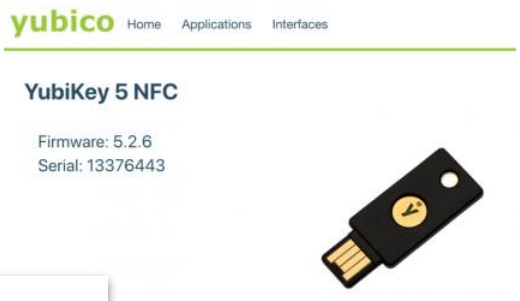
Not affected devices

- YubiKey 5 Nano
- YubiKey 5C
- YubiKey 5C Nano
- YubiKey 5Ci
- YubiKey FIPS Series
- Security Key Series
- YubiKey NEO
- YubiKey 4 Series

How to tell if you are affected

1. Identify your YubiKey. If you have a YubiKey 5 NFC continue to step 2. There are two ways to identify your key.

a. Use YubiKey Manager GUI to identify your key. The series and model of the key will be listed in the upper left corner of the Home screen. In the following example, the Yubikey is a 5 NFC.



YubiKey 5 NFC

Firmware: 5.2.6
Serial: 13376443

dentify your key based on the logo on the key. The YubiKey 5 NFC will feature the letter ectivity symbol above it inside of the gold circle on the front of the key, as pictured

2. Identify whether or not you have configured an access code following the steps below. Note: If your YubiKey was provided to you by an IT administrator or similar, contact your IT administrator for next steps.

a. Use the YubiKey Manager command line interface (CLI) to attempt to swap OTP slots.

```
$ ykman otp swap
```

b. If you receive the following error, it's likely you've configured an access code and you are affected by this issue.

```
Error: Failed to write to the YubiKey. Make sure the device does not have
restricted access.
```

c. If the command was successful, swap your OTP slots back.

```
$ ykman otp swap
```

Customer actions

If you followed the steps above and have identified that you are affected by this issue, there are several mitigation strategies that are available to you.

Mitigations

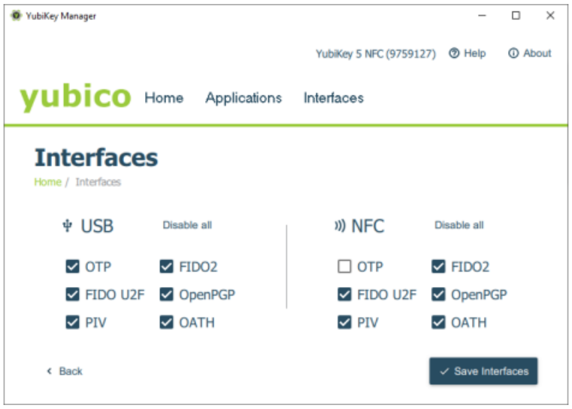
Disable OTP over NFC

If you use an access code and are not using OTP over NFC, disable the OTP application over NFC from the YubiKey Manager. This will still allow you to use the OTP application over USB and will still allow you to use other YubiKey applications such as FIDO2 and PIV (smart card) over NFC.

1 In YubiKey Manager select **Interfaces**

2 Uncheck **OTP** in the **NFC section**

3 Click **Save interfaces**



YubiKey Manager

YubiKey 5 NFC (9759127) Help About

yubico Home Applications Interfaces

Interfaces

Home / Interfaces

USB Disable all

☑ OTP ☑ FIDO2
☑ FIDO U2F ☑ OpenPGP
☑ PIV ☑ OATH

NFC Disable all

☐ OTP ☑ FIDO2
☑ FIDO U2F ☑ OpenPGP
☑ PIV ☑ OATH

‹ Back

✓ Save Interfaces

Note: If you are using an access code, and you also use OTP over NFC, we recommend reaching out to our support team for further assistance.

Rotate Static Password

If you are using the static password capability, you can rotate your password using the YubiKey Manager and following the steps outlined below. You may also want to consider using your YubiKey to hold part of the password and combine it with a portion of the password you remember.

1 In YubiKey Manager select **Applications**, then select **OTP** from the dropdown

2 Select **Configure** from the slot with your static password (Slot 1 or Slot 2)

3 Select **Static password** and click **Next**

4 Click **Generate** to generate a new password or enter the password you would like to set and to save your new password

letails

TP application provides two programmable slots that can each hold one credential of ypes: Yubico OTP, static password, HMAC-SHA1 challenge response, or OATH-HOTP. cation also allows users to set an access code to prevent unauthorized alteration of tion. To clarify, the access code does not protect against unauthorized access of the ts, it simply protects against unauthorized changes to your OTP configurations.

devices provide an NFC wireless interface in addition to USB. NFC Data Exchange) messages are sent to the YubiKey via USB or NFC to update NDEF records.

5.3.0 – 5.3.1, allows for possible changes to the
NFC without an access code check.

ed using NDEF?

n the slot. Typically, this is a URI that can be used by client applications to direct users to websites for authentication or information. This could potentially be altered so an application would send the OTP to a malicious site.

- Which slot is presented during an NFC read. By default, the OTP is configured in the first slot (often identified as the short-touch slot) and is presented over NFC. This can be altered so that the second slot is presented over NFC, even if a user has configured an access code.

Aggregate severity rating

Yubico has rated this issue as Moderate based on maximum security impact. The base CVSS score is 4.9