ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide additional situational awareness about a new security vulnerability found in several models of the YubiKey.

Why this matters

Yubikeys and YubiHSMs are extremely popular authentication devices used by individuals and organizations alike for the purpose of adding stronger security measures than a simple password can provide. While highly unlikely, a compromise of such a device could allow threat actors with physical access to a workstation easy access to its contents.

Overview

Recently, Yubico released an advisory[1] informing the public of a vulnerability within certain versions of their **Yubikey and YubiHSM** products that could allow an attacker **with physical access and specialised tooling** to get **access to the private keys** stored within.
Because these devices are configured at the factory and their firmware can never be altered past the initial installation, the only measure to patch the vulnerability is to acquire new Yubico devices.

The affected devices are:

Product Series	Affected Versions
YubiKey 5 Series	< 5.7
YubiKey 5 FIPS	< 5.7
YubiKey 5 CSPN	< 5.7
YubiKey Bio	< 5.7.2
Security Key	< 5.7
YubiHSM 2	< 2.4.0
YubiHSM 2 FIPS	< 2.4.0

To check the version of a particular Yubico product and validate whether it's affected:

- Yubikey:
  - Open the Yubico Authenticator app paired with the Yubikey;
  - The information will be in the upper left corner of the Home screen.

- YubiHSM:
  - Connect to the YubiHSM device via the YubiHSM SDK and execute the following commands:

```
  i.   $ yubihsm-connector -d
 ii.   $ yubihsm-shell
iii.   $ yubihsm> connect
 iv.   $ yubihsm> get deviceinfo
```

If none of the Yubico devices have affected firmware versions then no further action is required.

Recommendations

Recommendation #1: Conduct a risk assessment exercise

ORNA recommends that organizations with vulnerable devices assess the risks of maintaining the devices in use by estimating the chances of a targeted attack by an APT (Advanced Persistent Threat) or a nation state which can have physical access to the Yubico devices.

Recommendation #2: Upgrade the Yubico devices

ORNA **strongly recommends** that any organization at risk of being targeted by an APT with physical access to acquire new Yubico products in order to have devices with more recent firmware.

References

1. https://www.yubico.com/support/security-advisories/ysa-2024-03/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.
Sincerely,
ORNA Team