YubiKey – Infineon ECDSA Private Key Recovery

Overview

A vulnerability was discovered in Infineon's cryptographic library, potentially allowing an attacker with physical access to the YubiKey to recover affected private keys. This advisory references Yubico's YSA-2024-03 security advisory.

Affected Products and Versions

All YubiKey 5 Series Keys versions < 5.7

Note: To identify the YubiKey, use Yubico Authenticator to identify the model and version of the YubiKey. The series and model of the key will be listed in the upper left corner of the Home screen.

Vulnerability Details

ISSUE	BASE SCORE	ADJUSTED SCORE	PLATFORM	DESCRIPTION
ISSUE 1	4.9 (Medium)	3.6 (Low)	YubiKey 5 Series Key	Side-Channel Key Recovery

Note: Adjusted Score is an environmental score calculated according to impact with regards to compensating controls and overall system impact in the customer environment.

An attacker could exploit this issue as part of a sophisticated and targeted attack to recover affected private keys. The attacker would need physical possession of the YubiKey, Security Key, or YubiHSM, knowledge of the accounts they want to target, and specialized equipment to perform the necessary attack. Depending on the use case, the attacker may also require additional knowledge including username, PIN, account password, or authentication key.

This vulnerability will impact Gas Power customers with Xona devices and those using YubiKey authentication for certain HMI deployments.

Exploitation Status

GE Vernova has not yet observed or received reports of any Gas Power customer equipment being compromised by this vulnerability.

Remediation/Mitigation

Full remediation of this issue would require replacement of existing YubiKeys with YubiKey 5.7; however, as the impact of this issue is low and requires an attacker to gain physical access to an affected YubiKey, GE Vernova is not recommending any specific action.

For customers that would prefer to remediate this issue directly, please reach out to your local GE Vernova Services representative for support in replacing your existing YubiKeys.

Contact Information

Contact your local GE Vernova Services representative for assistance or additional information.
For Product Security issues or incident/vulnerability reporting: https://www.gevernova.com/security

Document History

Version	Release Date	Purpose
1.0	10/28/2024	Initial Release

Disclaimer

Unless the product is under a GE Vernova service contract, GE Vernova assumes no responsibility or liability for the content of Security Notices or for making Security Notices available to customer. Implementing Security Notices as well as performing updates/upgrades to software/firmware is solely the responsibility of the customer.