CVE-2020-10185

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-10185
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-05 23:15:00 UTC
Updated	2020-03-12 23:15:00 UTC
Description	The sync endpoint in YubiKey Validation Server before 2.40 allows remote attackers to replay an OTP. NOTE: this issue is

Risk And Classification

Problem Types: CWE-294

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yubico	Yubikey One Time Password Validation Server	All	All	All	All
Application	Yubico	Yubikey One Time Password Validation Server	All	All	All	All

References

Reference	Source	Link
Security advisory 2020-03-03 | Yubico	MISC	www.yu
Release yubikey-val-2.40: Merge pull request #59 from Yubico/enhance_data_validation · Yubico/yubikey-val · GitHub	MISC	github.c
[SECURITY] [DLA 2141-1] yubikey-val security update	MLIST	lists.deb
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

CVE.report and Source URL Uptime Status status.cve.report