Tillitis: TKey Client has an Error in Protocol Implementation

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-32953
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-20 05:16:14 UTC
Updated	2026-04-16 13:14:09 UTC
Description	Tillitis TKey Client package is a Go package for a TKey client. Versions 1.2.0 and below contain a critical bug in the tkeyclie

Risk And Classification

Primary CVSS: v4.0 4.7 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000060000 probability, percentile 0.003410000 (date 2026-04-21)

Problem Types: CWE-303 | NVD-CWE-noinfo | CWE-303 CWE-303: Incorrect Implementation of Authentication Algorithm

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	4.7	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:H/S
4.0	CNA	DECLARED	4.7	MEDIUM	CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:H/S
3.1	nvd@nist.gov	Primary	4.6	MEDIUM	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Low

Integrity

Low

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:H/SI:H/SA:H/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

None

CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tillitis	Tkey Client	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

Source	Vendor	Product	Version	Platforms
CNA	Tillitis	Tkeyclient	affected < 1.3.0	Not specified

References

Reference	Source	Link	Tags
github.com/tillitis/tkeyclient/releases/tag/v1.3.0	security-advisories@github.com	github.com	Release No
github.com/tillitis/tkeyclient/security/advisories/GHSA-4w7r-3222-8h6v	security-advisories@github.com	github.com	Exploit, Ven
github.com/tillitis/tkeyclient/commit/4954dccf0287657edf8d405057e134cdff...	security-advisories@github.com	github.com	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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