janmojzis tinyssh Ed25519 Signature crypto_sign_ed25519_tinyssh.c signature verification

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

Summary

CVE	CVE-2026-4541
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-22 09:15:59 UTC
Updated	2026-04-18 05:16:22 UTC
Description	A flaw has been found in janmojzis tinyssh up to 20250501. Impacted is an unknown function of the file tinyssh/crypto_sign_

Risk And Classification

Primary CVSS: v4.0 2 LOW from cna@vuldb.com

CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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: 0.000020000 probability, percentile 0.000330000 (date 2026-04-21)

Problem Types: CWE-345 | CWE-347 | CWE-347 Improper Verification of Cryptographic Signature | CWE-345 Insufficient Verification of Data Authenticity

Version	Source	Type	Score	Severity	Vector
4.0	cna@vuldb.com	Secondary	2	LOW	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/C...
4.0	CNA	DECLARED	2	LOW	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Secondary	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
3.0	CNA	DECLARED	2.5	LOW	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	1		AV:L/AC:H/Au:S/C:N/I:P/A:N
2.0	CNA	DECLARED	1		AV:L/AC:H/Au:S/C:N/I:P/A:N/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

None

Privileges Required

Low

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/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

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Janmojzis	Tinyssh	affected 20250501	Not specified
CNA	Janmojzis	Tinyssh	unaffected 20260301	Not specified

References

Reference	Source	Link	Tags
github.com/janmojzis/tinyssh/issues/101	cna@vuldb.com	github.com	
github.com/janmojzis/tinyssh/pull/102	cna@vuldb.com	github.com	
vuldb.com/submit/774687	cna@vuldb.com	vuldb.com	
vuldb.com/vuln/352358	cna@vuldb.com	vuldb.com	
github.com/janmojzis/tinyssh/commit/9c87269607e0d7d20174df742accc49c042c...	cna@vuldb.com	github.com	
github.com/janmojzis/tinyssh/issues/101	cna@vuldb.com	github.com	
github.com/janmojzis/tinyssh/releases/tag/20260301	cna@vuldb.com	github.com	
vuldb.com/vuln/352358/cti	cna@vuldb.com	vuldb.com	
github.com/janmojzis/tinyssh	cna@vuldb.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: pythok (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-01T00:00:00.000Z	Countermeasure disclosed
CNA	2026-03-21T00:00:00.000Z	Advisory disclosed
CNA	2026-03-21T01:00:00.000Z	VulDB entry created
CNA	2026-03-23T05:12:55.000Z	VulDB entry last update

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