PuTTY Ed25519 Signature ecc-ssh.c eddsa_verify signature verification

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

Summary

CVE	CVE-2026-4115
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-22 13:16:20 UTC
Updated	2026-04-30 18:33:16 UTC
Description	A vulnerability was detected in PuTTY 0.83. Affected is the function eddsa_verify of the file crypto/ecc-ssh.c of the compone

Risk And Classification

Primary CVSS: v4.0 2.9 LOW from cna@vuldb.com

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/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: 0.000170000 probability, percentile 0.043760000 (date 2026-05-05)

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	2.9	LOW	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P/C.
4.0	CNA	DECLARED	6.3	MEDIUM	CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:P
3.1	cna@vuldb.com	Primary	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
3.1	CNA	DECLARED	3.7	LOW	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
3.0	CNA	DECLARED	3.7	LOW	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
2.0	cna@vuldb.com	Secondary	2.6		AV:N/AC:H/Au:N/C:N/I:P/A:N
2.0	CNA	DECLARED	2.6		AV:N/AC:H/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

None

Integrity

Low

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:H/AT:N/PR:N/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

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

Low

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Putty	Putty	0.83	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	PuTTY	affected 0.83	Not specified

References

Reference	Source	Link	Tags
www.rfc-editor.org/rfc/rfc8032	cna@vuldb.com	www.rfc-editor.org	Technical D
github.com/py-thok/putty-ed25519-malleability-s-plus-l/blob/main/poc.py	cna@vuldb.com	github.com	Exploit
vuldb.com	cna@vuldb.com	vuldb.com	Third Party
git.tartarus.org	cna@vuldb.com	git.tartarus.org	Permissions
www.chiark.greenend.org.uk/~sgtatham/putty/wishlist/eddsa-overlarge-s.html	cna@vuldb.com	www.chiark.greenend.org.uk	Third Party
github.com/py-thok/putty-ed25519-malleability-s-plus-l	cna@vuldb.com	github.com	Third Party
vuldb.com	cna@vuldb.com	vuldb.com	Third Party
vuldb.com	cna@vuldb.com	vuldb.com	Permissions
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

Vendor Comments And Credit

Discovery Credit

CNA: pythok (VulDB User) (en)

CNA: VulDB (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-22T00:00:00.000Z	Advisory disclosed
CNA	2026-03-22T01:00:00.000Z	VulDB entry created
CNA	2026-03-22T12:54:35.000Z	VulDB entry last update

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