mkj Dropbear S Range Check curve25519.c unpackneg signature verification

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

Summary

CVE	CVE-2026-3706
State	PUBLISHED
Assigner	VulDB
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-08 05:16:31 UTC
Updated	2026-04-22 21:27:27 UTC
Description	A vulnerability was determined in mkj Dropbear up to 2025.89. Impacted is the function unpackneg of the file src/curve2551

Risk And Classification

Primary CVSS: v4.0 1.7 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:U/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 0.003450000 (date 2026-04-22)

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	1.7	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:U/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:U
3.1	cna@vuldb.com	Secondary	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:U/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:U/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:U/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:U/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:U/RL:O/RC:C

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Mkj	Dropbear	affected 2025.0	Not specified
CNA	Mkj	Dropbear	affected 2025.1	Not specified
CNA	Mkj	Dropbear	affected 2025.2	Not specified
CNA	Mkj	Dropbear	affected 2025.3	Not specified
CNA	Mkj	Dropbear	affected 2025.4	Not specified
CNA	Mkj	Dropbear	affected 2025.5	Not specified
CNA	Mkj	Dropbear	affected 2025.6	Not specified
CNA	Mkj	Dropbear	affected 2025.7	Not specified
CNA	Mkj	Dropbear	affected 2025.8	Not specified
CNA	Mkj	Dropbear	affected 2025.9	Not specified
CNA	Mkj	Dropbear	affected 2025.10	Not specified
CNA	Mkj	Dropbear	affected 2025.11	Not specified
CNA	Mkj	Dropbear	affected 2025.12	Not specified
CNA	Mkj	Dropbear	affected 2025.13	Not specified
CNA	Mkj	Dropbear	affected 2025.14	Not specified
CNA	Mkj	Dropbear	affected 2025.15	Not specified
CNA	Mkj	Dropbear	affected 2025.16	Not specified
CNA	Mkj	Dropbear	affected 2025.17	Not specified
CNA	Mkj	Dropbear	affected 2025.18	Not specified

CNA	Mkj	Dropbear	affected 2025.19	Not specified
CNA	Mkj	Dropbear	affected 2025.20	Not specified
CNA	Mkj	Dropbear	affected 2025.21	Not specified
CNA	Mkj	Dropbear	affected 2025.22	Not specified
CNA	Mkj	Dropbear	affected 2025.23	Not specified
CNA	Mkj	Dropbear	affected 2025.24	Not specified
CNA	Mkj	Dropbear	affected 2025.25	Not specified
CNA	Mkj	Dropbear	affected 2025.26	Not specified
CNA	Mkj	Dropbear	affected 2025.27	Not specified
CNA	Mkj	Dropbear	affected 2025.28	Not specified
CNA	Mkj	Dropbear	affected 2025.29	Not specified
CNA	Mkj	Dropbear	affected 2025.30	Not specified
CNA	Mkj	Dropbear	affected 2025.31	Not specified
CNA	Mkj	Dropbear	affected 2025.32	Not specified
CNA	Mkj	Dropbear	affected 2025.33	Not specified
CNA	Mkj	Dropbear	affected 2025.34	Not specified
CNA	Mkj	Dropbear	affected 2025.35	Not specified
CNA	Mkj	Dropbear	affected 2025.36	Not specified
CNA	Mkj	Dropbear	affected 2025.37	Not specified
CNA	Mkj	Dropbear	affected 2025.38	Not specified
CNA	Mkj	Dropbear	affected 2025.39	Not specified
CNA	Mkj	Dropbear	affected 2025.40	Not specified
CNA	Mkj	Dropbear	affected 2025.41	Not specified
CNA	Mkj	Dropbear	affected 2025.42	Not specified
CNA	Mkj	Dropbear	affected 2025.43	Not specified
CNA	Mkj	Dropbear	affected 2025.44	Not specified
CNA	Mkj	Dropbear	affected 2025.45	Not specified
CNA	Mkj	Dropbear	affected 2025.46	Not specified
CNA	Mkj	Dropbear	affected 2025.47	Not specified
CNA	Mkj	Dropbear	affected 2025.48	Not specified
CNA	Mkj	Dropbear	affected 2025.49	Not specified
CNA	Mkj	Dropbear	affected 2025.50	Not specified
CNA	Mkj	Dropbear	affected 2025.51	Not specified
CNA	Mkj	Dropbear	affected 2025.52	Not specified
CNA	Mkj	Dropbear	affected 2025.53	Not specified

CNA	Mkj	Dropbear	affected 2025.54	Not specified
CNA	Mkj	Dropbear	affected 2025.55	Not specified
CNA	Mkj	Dropbear	affected 2025.56	Not specified
CNA	Mkj	Dropbear	affected 2025.57	Not specified
CNA	Mkj	Dropbear	affected 2025.58	Not specified
CNA	Mkj	Dropbear	affected 2025.59	Not specified
CNA	Mkj	Dropbear	affected 2025.60	Not specified
CNA	Mkj	Dropbear	affected 2025.61	Not specified
CNA	Mkj	Dropbear	affected 2025.62	Not specified
CNA	Mkj	Dropbear	affected 2025.63	Not specified
CNA	Mkj	Dropbear	affected 2025.64	Not specified
CNA	Mkj	Dropbear	affected 2025.65	Not specified
CNA	Mkj	Dropbear	affected 2025.66	Not specified
CNA	Mkj	Dropbear	affected 2025.67	Not specified
CNA	Mkj	Dropbear	affected 2025.68	Not specified
CNA	Mkj	Dropbear	affected 2025.69	Not specified
CNA	Mkj	Dropbear	affected 2025.70	Not specified
CNA	Mkj	Dropbear	affected 2025.71	Not specified
CNA	Mkj	Dropbear	affected 2025.72	Not specified
CNA	Mkj	Dropbear	affected 2025.73	Not specified
CNA	Mkj	Dropbear	affected 2025.74	Not specified
CNA	Mkj	Dropbear	affected 2025.75	Not specified
CNA	Mkj	Dropbear	affected 2025.76	Not specified
CNA	Mkj	Dropbear	affected 2025.77	Not specified
CNA	Mkj	Dropbear	affected 2025.78	Not specified
CNA	Mkj	Dropbear	affected 2025.79	Not specified
CNA	Mkj	Dropbear	affected 2025.80	Not specified
CNA	Mkj	Dropbear	affected 2025.81	Not specified
CNA	Mkj	Dropbear	affected 2025.82	Not specified
CNA	Mkj	Dropbear	affected 2025.83	Not specified
CNA	Mkj	Dropbear	affected 2025.84	Not specified
CNA	Mkj	Dropbear	affected 2025.85	Not specified
CNA	Mkj	Dropbear	affected 2025.86	Not specified
CNA	Mkj	Dropbear	affected 2025.87	Not specified
CNA	Mkj	Dropbear	affected 2025.88	Not specified

CNA	Mkj	Dropbear	affected 2025.89	Not specified

References

Reference	Source	Link
vuldb.com	cna@vuldb.com	vuldb.com
vuldb.com	cna@vuldb.com	vuldb.com
github.com/mkj/dropbear/commit/fdec3c90a15447bd538641d85e5a3e3ac981011d	cna@vuldb.com	github.com
github.com/mkj/dropbear/issues/406	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com
github.com/mkj/dropbear	cna@vuldb.com	github.com
github.com/str4d/ed25519-java/issues/82	cna@vuldb.com	github.com
vuldb.com	cna@vuldb.com	vuldb.com
github.com/mkj/dropbear/pull/407	cna@vuldb.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: pythok (VulDB User) (en)

Additional Advisory Data

Source	Time	Event
CNA	2026-03-07T00:00:00.000Z	Advisory disclosed
CNA	2026-03-07T01:00:00.000Z	VulDB entry created
CNA	2026-03-16T06:42:50.000Z	VulDB entry last update

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