CVE-2017-11104

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

Summary

CVE	CVE-2017-11104
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-08 10:29:00 UTC
Updated	2023-01-20 15:23:00 UTC
Description	Knot DNS before 2.4.5 and 2.5.x before 2.5.2 contains a flaw within the TSIG protocol implementation that would allow an a

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Knot-dns	Knot Dns	2.5.0	All	All	All
Application	Knot-dns	Knot Dns	2.5.1	All	All	All
Application	Knot-dns	Knot Dns	2.5.0	All	All	All
Application	Knot-dns	Knot Dns	2.5.1	All	All	All
Application	Knot-dns	Knot Dns	All	All	All	All

References

Reference	Source	Link
[security-announce] openSUSE-SU-2020:1232-1: moderate: Security update f	SUSE	lists.c
#865678 - knot: CVE-2017-11104: Improper TSIG validity period check can allow TSIG forgery - Debian Bug report logs	MISC	bugs.
[knot-dns-users] Knot DNS 2.5.2 and 2.4.5 releases	MISC	lists.r
Debian -- Security Information -- DSA-3910-1 knot	DEBIAN	www.
[security-announce] openSUSE-SU-2020:1086-1: moderate: Security update f	SUSE	lists.c
Malformed Request	BID	www.

www.synacktiv.ninja/ressources/Knot_DNS_TSIG_Signature_Forgery.pdf	MISC	www.
[security-announce] openSUSE-SU-2020:1085-1: moderate: Security update f	SUSE	lists.c
[security-announce] openSUSE-SU-2020:1112-1: moderate: Security update f	SUSE	lists.c
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

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