CVE-2014-4883

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

Summary

CVE	CVE-2014-4883
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-11-28 02:59:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	resolv.c in the DNS resolver in uIP, and dns.c in the DNS resolver in lwIP 1.4.1 and earlier, does not use random values for

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-345 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lwip Project	Lwip	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Vulnerability Note VU#210620 - uIP and lwIP DNS resolver vulnerable to cache poisoning	af854a3a-2127-422b-91ae-364da2661108	www
lwip.git - lwIP - A Lightweight TCPIP stack	af854a3a-2127-422b-91ae-364da2661108	git.s
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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