CVE-2010-2522

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

Summary

CVE	CVE-2010-2522
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-07-13 17:30:04 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The mipv6 daemon in UMIP 0.4 does not verify that netlink messages originated in the kernel, which allows local users to s

Risk And Classification

Primary CVSS: v2.0 2.1 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linux-ipv6	Umip	0.4	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Usagi Project mipv6-daemon Unicast Kernel Message Spoofing Vulnerability	af854a3a-2127-422b-91ae-364
'Re: [oss-security] patch for remote buffer overflows and local' - MARC	af854a3a-2127-422b-91ae-364
'[oss-security] Re: patch for remote buffer overflows and local message spoofing in mipv6 daemon' - MARC	af854a3a-2127-422b-91ae-364
oss-security - Re: patch for remote buffer overflows and local message spoofing in mipv6 daemon	af854a3a-2127-422b-91ae-364
oss-security - patch for remote buffer overflows and local message spoofing in mipv6 daemon	af854a3a-2127-422b-91ae-364
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:019	af854a3a-2127-422b-91ae-364
oss-security - Re: patch for remote buffer overflows and local message spoofing in mipv6 daemon	af854a3a-2127-422b-91ae-364
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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