CVE-2009-2073

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

Summary

CVE	CVE-2009-2073
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-15 19:30:05 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Cross-site request forgery (CSRF) vulnerability in Linksys WRT160N wireless router hardware 1 and firmware 1.02.2 allows

Risk And Classification

Primary CVSS: v2.0 6.8 from nvd@nist.gov

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

Problem Types: CWE-352 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Wrt160n	1.02.2	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
holisticinfosec.org - HIO-2009-0405 Linksys WRT160N CSRF	af854a3a-2127-
Linksys WRT160N Wireless Router Cross-Site Request Forgery Vulnerability	af854a3a-2127-
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-
IBM X-Force Exchange	af854a3a-2127-
Linksys WRT160N Cross-Site Request Forgery Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-
www.osvdb.org/53414	af854a3a-2127-
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.