CVE-2008-2636

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

Summary

CVE	CVE-2008-2636
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-06-10 00:32:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The HTTP service on the Cisco Linksys WRH54G with firmware 1.01.03 allows remote attackers to cause a denial of servic

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Linksys Wrh54g Router	1.01.03	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
IBM X-Force Exchange	af854a3a-2127-422b-91ae-
Linksys WRH54G Router Management Interface Can Be Crashed By Remote Users - SecurityTracker	af854a3a-2127-422b-91ae-
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-
Linksys WRH54G Denial of Service Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-
SecurityReason - Remote DoS vulnerability in Linksys WRH54G	af854a3a-2127-422b-91ae-
SecurityFocus	af854a3a-2127-422b-91ae-
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.