CVE-2005-1680

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

Summary

CVE	CVE-2005-1680
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-20 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	D-Link DSL-502T, DSL-504T, DSL-562T, and DSL-G604T, when /cgi-bin/firmwarecfg is executed, allows remote attackers

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dsl-502t	All	All	All	All

Hardware	D-link	Dsl-504t	All	All	All	All
Hardware	D-link	Dsl-562t	All	All	All	All
Hardware	D-link	Dsl-g604t	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	Tags
'D-Link DSL routers authentication bypass' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108	www.vupen.com	
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

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