CVE-2005-1827

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

Summary

CVE	CVE-2005-1827
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-05-26 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	D-Link DSL-504T allows remote attackers to bypass authentication and gain privileges, such as upgrade firmware, restart tl

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: CWE-425 | 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	Dlink	Dsl-504t	-	All	All	All

Operating System	Dlink	Dsl-504t Firmware	1.00b01t16.eu.20040217	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
Secunia - Advisories - D-Link DSL Routers "firmwarecfg" Authentication Bypass	af854a3a-2127-422b-91ae-364da2661108	secunia.cc
'DSL-504T (and maybe many other) remote access without password bug' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.info
D-Link DSL Router Remote Authentication Bypass Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.secu
CVE Program record	CVE.ORG	www.cve.c
NVD vulnerability detail	NVD	nvd.nist.gc

No vendor comments have been submitted for this CVE.

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