



CVE-2002-1069

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2002-1069
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-10-04 04:00:00 UTC
Updated	2016-10-18 02:23:00 UTC
Description	The remote administration capability for the D-Link DI-804 router 4.68 allows remote attackers to bypass authentication and

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Di-804	4.68	All	All	All
Hardware	D-link	Di-804	4.68	All	All	All

References

Reference

- ISS X-Force Database: dlink-admin-dhcp-release (9967): D-Link DI-804 router "Remote Administration" allows unauthorized release/renew of
- ISS X-Force Database: dlink-admin-device-information (9969): D-Link DI-804 router "Remote Administration" allows remote attacker to obtain
- D-Link Remote Administration Information Leakage Vulnerability
- SecurityFocus HOME Mailing List: BugTraq
- 'Re: possible exploit: D-Link DI-804 unauthorized DHCP release' - MARC
- D-Link Remote Administration Arbitrary DHCP Address Release Vulnerability
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)