



# CVE-2018-10822

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

## Summary

<b>CVE</b>	CVE-2018-10822
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-10-17 14:29:00 UTC
<b>Updated</b>	2023-11-08 22:46:00 UTC
<b>Description</b>	Directory traversal vulnerability in the web interface on D-Link DWR-116 through 1.06, DIR-140L through 1.02, DIR-640L th

## Risk And Classification

### Problem Types: CWE-22

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	<a href="#">D-link</a>	<a href="#">Dir-140l</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-140l</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dir-140l Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-640l</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dir-640l</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dir-640l Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-111</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-111</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dwr-111 Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-116</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-116</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dwr-116 Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-512</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-512</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dwr-512 Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-712</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-712</a>	-	All	All	All

Operating System	<a href="#">D-link</a>	<a href="#">Dwr-712 Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-912</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-912</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dwr-912 Firmware</a>	All	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-921</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-921</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dwr-921 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-140I</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dir-140I Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dir-640I</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dir-640I Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dwr-111</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dwr-111 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dwr-116</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dwr-116 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dwr-512</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dwr-512 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dwr-712</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dwr-712 Firmware</a>	All	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dwr-912 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dwr-921</a>	-	All	All	All
Operating System	<a href="#">Dlink</a>	<a href="#">Dwr-921 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
D-Link routers - full takeover	MISC	<a href="#">sploit.tech</a>	Exploit
Full Disclosure: Multiple vulnerabilities in D-Link routers	FULLDISC	<a href="#">seclists.org</a>	Exploit, Mailing List, Third Party Advisory
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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](#).

**Free CVE JSON API** [cve.report/api](#)

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