



CVE-2016-5681

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

Summary

CVE	CVE-2016-5681
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-25 21:59:00 UTC
Updated	2023-06-26 19:38:00 UTC
Description	Stack-based buffer overflow in dws/api/Login on D-Link DIR-850L B1 2.07 before 2.07WWB05, DIR-817 Ax, DIR-818LW B...

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dir-817lw	ax	All	All	All
Operating System	D-link	Dir-817lw Firmware	All	All	All	All
Hardware	D-link	Dir-817lw	ax	All	All	All
Hardware	D-link	Dir-817lw	ax	All	All	All
Operating System	D-link	Dir-817lw Firmware	All	All	All	All
Hardware	D-link	Dir-818lw	ax	All	All	All
Operating System	D-link	Dir-818lw Firmware	All	All	All	All
Hardware	D-link	Dir-818lw	ax	All	All	All
Hardware	D-link	Dir-818lw	ax	All	All	All
Operating System	D-link	Dir-818lw Firmware	All	All	All	All
Hardware	D-link	Dir-822	a1	All	All	All
Hardware	D-link	Dir-822	a1	All	All	All
Hardware	D-link	Dir-822 Firmware	3.01	All	All	All
Hardware	D-link	Dir-822 Firmware	3.01	All	All	All
Hardware	D-link	Dir-823	a1	All	All	All
Hardware	D-link	Dir-823	a1	All	All	All
Operating System	D-link	Dir-823 Firmware	All	All	All	All

Hardware	D-link	Dir-850l	b1	All	All	All
Hardware	D-link	Dir-850l	b1	All	All	All
Operating System	D-link	Dir-850l Firmare	All	All	All	All
Hardware	D-link	Dir-868l	b1	All	All	All
Hardware	D-link	Dir-868l	c1	All	All	All
Hardware	D-link	Dir-868l	b1	All	All	All
Hardware	D-link	Dir-868l	c1	All	All	All
Operating System	D-link	Dir-868l Firmware	All	All	All	All
Operating System	D-link	Dir-868l Firmware	All	All	All	All
Hardware	D-link	Dir-880l	a1	All	All	All
Hardware	D-link	Dir-880l	a1	All	All	All
Operating System	D-link	Dir-880l Firmware	All	All	All	All
Hardware	D-link	Dir-885l	a1	All	All	All
Hardware	D-link	Dir-885l	a1	All	All	All
Operating System	D-link	Dir-885l Firmware	All	All	All	All
Hardware	D-link	Dir-890l	a1	All	All	All
Hardware	D-link	Dir-890l	a1	All	All	All
Operating System	D-link	Dir-890l Firmware	All	All	All	All
Hardware	D-link	Dir-895l	a1	All	All	All
Hardware	D-link	Dir-895l	a1	All	All	All
Operating System	D-link	Dir-895l Firmware	All	All	All	All
Hardware	Dlink	Dir-817lw	ax	All	All	All
Hardware	Dlink	Dir-818lw	ax	All	All	All
Hardware	Dlink	Dir-822	a1	All	All	All
Operating System	Dlink	Dir-822 Firmware	3.01	All	All	All
Hardware	Dlink	Dir-823	a1	All	All	All
Hardware	Dlink	Dir-850l	b1	All	All	All
Hardware	Dlink	Dir-868l	b1	All	All	All
Hardware	Dlink	Dir-868l	c1	All	All	All
Operating System	Dlink	Dir-868l Firmware	All	All	All	All
Operating System	Dlink	Dir-868l Firmware	All	All	All	All
Hardware	Dlink	Dir-880l	a1	All	All	All
Hardware	Dlink	Dir-885l	a1	All	All	All
Hardware	Dlink	Dir-890l	a1	All	All	All
Hardware	Dlink	Dir-895l	a1	All	All	All

References

Reference	Source	Link	Tags
Multiple D-Link Routers CVE-2016-5681 Stack Based Buffer Overflow Vulnerability	BID	www.securityfocus.com	
Vulnerability Note VU#332115 - D-Link routers contain buffer overflow vulnerability	CERT-VN	www.kb.cert.org	Third
D-Link Technical Support	CONFIRM	supportannouncement.us.dlink.com	Venc
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report