



# CVE-2018-19300

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-19300
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-04-11 16:29:00 UTC
<b>Updated</b>	2023-04-26 19:27:00 UTC
<b>Description</b>	On D-Link DAP-1530 (A1) before firmware version 1.06b01, DAP-1610 (A1) before firmware version 1.06b01, DWR-111 (A

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dap-1530	-	All	All	All
Hardware	D-link	Dap-1530	-	All	All	All
Operating System	D-link	Dap-1530 Firmware	All	All	All	All
Hardware	D-link	Dap-1610	-	All	All	All
Hardware	D-link	Dap-1610	-	All	All	All
Operating System	D-link	Dap-1610 Firmware	All	All	All	All
Hardware	D-link	Dwr-111	-	All	All	All
Hardware	D-link	Dwr-111	-	All	All	All
Operating System	D-link	Dwr-111 Firmware	All	All	All	All
Hardware	D-link	Dwr-116	-	All	All	All
Hardware	D-link	Dwr-116	-	All	All	All
Operating System	D-link	Dwr-116 Firmware	1.06	b1	All	All
Operating System	D-link	Dwr-116 Firmware	1.06	b2	All	All
Operating System	D-link	Dwr-116 Firmware	1.06	b1	All	All
Operating System	D-link	Dwr-116 Firmware	1.06	b2	All	All
Operating System	D-link	Dwr-116 Firmware	All	All	All	All
Hardware	D-link	Dwr-512	-	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-711</a>	-	All	All	All
Hardware	<a href="#">D-link</a>	<a href="#">Dwr-711</a>	-	All	All	All
Operating System	<a href="#">D-link</a>	<a href="#">Dwr-711 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-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
Operating System	<a href="#">D-link</a>	<a href="#">Dwr-921 Firmware</a>	All	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dap-1530</a>	-	All	All	All
Hardware	<a href="#">Dlink</a>	<a href="#">Dap-1610</a>	-	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-711</a>	-	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
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
Operating System	<a href="#">Dlink</a>	<a href="#">Dwr-921 Firmware</a>	All	All	All	All

## References

### Reference

[Serious vulnerability discovered in D-Link routers - Greenbone Networks](#)

[Schwachstelle durch Command Execution in D-Link DWR und DAP Routern \(/EXCU\\_SHELL\) | D-Link Deutschland](#)

[CVE-2018-19300: Remote Command Execution Vulnerability in D-Link DWR and DAP Routers - Vulnerability Tests - Greenbone Community](#)

[Schwerwiegende Sicherheitslücke in D-Link-Routern entdeckt - Greenbone Networks](#)

[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](#).

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

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