



CVE-2006-6538

Published on: 12/13/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:04 PM UTC

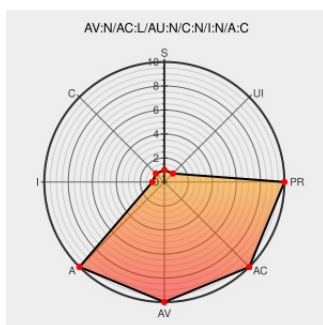
CVE-2006-6538

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Dwl-2000ap](#) from [D-link](#) contain the following vulnerability:

D-LINK DWL-2000AP+ firmware 2.11 allows remote attackers to cause (1) a denial of service (device reset) via a flood of ARP replies on the wired or wireless (radio) link and (2) a denial of service (device crash) via a flood of ARP requests on the wireless link.

CVE-2006-6538 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.8 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

www.vupen.com
[text/html](#)

[VUPEN ADV-2006-4965](#)

[Exploit](#)
tripp.dynalias.org
[text/x-c](#)
[Inactive Link](#) [Not Archived](#)

[MISC tripp.dynalias.org/arpflood.c](http://misc.tripp.dynalias.org/arpflood.c)

D-LINK DWL-2000AP+ Denial of Service - Advisories - Secunia

web.archive.org
[text/html](#)

[SECUNIA 23332](#)

SecurityFocus

www.securityfocus.com
[text/html](#)

[BUGTRAQ 20061211 D-LINK DWL-2000AP+ remote DoS](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
[text/html](#)

[XF dlink-arp-dos\(30837\)](#)

D-Link DWL-2000AP 2.11 (ARP Flood) Remote Denial of Service Exploit

www.exploit-db.com

Proof of Concept

text/x-c

 EXPLOIT-DB 2915

SecurityReason - D-LINK DWL-2000AP+ remote DoS

securityreason.com

text/html

 SREASON 2029

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	D-link	Dwl-2000ap	2.11	All	All	All
Hardware 	D-link	Dwl-2000ap	2.11	All	All	All
Hardware 	D-link	Dwl-2000ap	2.11	All	All	All
cpe:2.3:h:d-link:dwl-2000ap+:2.11:~::~~::~~::						
cpe:2.3:h:d-link:dwl-2000ap\+:2.11:~::~~::~~::						
cpe:2.3:h:d-link:dwl-2000ap\+:2.11:~::~~::~~::						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023 

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](#)