



CVE-2006-6055

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

Summary

CVE	CVE-2006-6055
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-11-22 01:07:00 UTC
Updated	2011-03-08 02:44:00 UTC
Description	Stack-based buffer overflow in A5AGU.SYS 1.0.1.41 for the D-Link DWL-G132 wireless adapter allows remote attackers to

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	Dwl-g132	All	All	All	All
Hardware	D-link	Dwl-g132	All	All	All	All

References

Reference	Source
SecurityTracker.com Archives - D-Link DWL-G132 Wireless USB Adapter Stack Overflow Lets Remote Users Execute Arbitrary Code	SECURITY
Month of Kernel Bugs (MoKB): D-Link DWL-G132 Wireless Driver Beacon Rates Overflow	MISC
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VULNERABILITY
D-Link DWL-G132 ASAGU.SYS Wireless Device Driver Stack Buffer Overflow Vulnerability	BID
D-Link DWL-G132 Wireless Driver Beacon Rates Buffer Overflow - Advisories - Secunia	SECURITY
CVE Program record	CVE
NVD vulnerability detail	NVD

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](#)