



CVE-2006-6125

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

Summary

CVE	CVE-2006-6125
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-11-27 00:07:00 UTC
Updated	2011-10-17 04:00:00 UTC
Description	Heap-based buffer overflow in the wireless driver (WG311ND5.SYS) 2.3.1.10 for NetGear WG311v1 wireless adapter allow

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Netgear	Wg311v1	2.3.1.10	All	All	All
Hardware	Netgear	Wg311v1	2.3.1.10	All	All	All

References

Reference	Source
Month of Kernel Bugs (MoKB): NetGear WG311v1 Wireless Driver Long SSID Overflow	MIS
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUF
SecurityTracker.com Archives - Netgear WG311v1 Wireless Adapter SSID Buffer Overflow Lets Remote Users Execute Arbitrary Code	SEC
US-CERT Vulnerability Note VU#403152	CEF
NetGear WG311v1 Wireless Driver Long SSID Buffer Overflow - Advisories - Secunia	SEC
NetGear WG311v1 Wireless Driver SSID Heap Buffer Overflow Vulnerability	BID
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](#)