



CVE-2007-6201

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

Summary

CVE	CVE-2007-6201
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-01 06:46:00 UTC
Updated	2017-07-29 01:34:00 UTC
Description	Unspecified vulnerability in Wesnoth 1.2.x before 1.2.8, and 1.3.x before 1.3.12, allows attackers to cause a denial of service

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wesnoth	Wesnoth	1.2	All	All	All
Application	Wesnoth	Wesnoth	1.2.1	All	All	All
Application	Wesnoth	Wesnoth	1.2.2	All	All	All
Application	Wesnoth	Wesnoth	1.2.3	All	All	All
Application	Wesnoth	Wesnoth	1.2.4	All	All	All
Application	Wesnoth	Wesnoth	1.2.5	All	All	All
Application	Wesnoth	Wesnoth	1.2.6	All	All	All
Application	Wesnoth	Wesnoth	1.2.7	All	All	All
Application	Wesnoth	Wesnoth	1.3.1	All	All	All
Application	Wesnoth	Wesnoth	1.3.10	All	All	All
Application	Wesnoth	Wesnoth	1.3.11	All	All	All
Application	Wesnoth	Wesnoth	1.3.2	All	All	All
Application	Wesnoth	Wesnoth	1.3.3	All	All	All
Application	Wesnoth	Wesnoth	1.3.4	All	All	All
Application	Wesnoth	Wesnoth	1.3.5	All	All	All
Application	Wesnoth	Wesnoth	1.3.6	All	All	All
Application	Wesnoth	Wesnoth	1.3.7	All	All	All

Application	Wesnoth	Wesnoth	1.3.8	All	All	All
Application	Wesnoth	Wesnoth	1.3.9	All	All	All
Application	Wesnoth	Wesnoth	1.2	All	All	All
Application	Wesnoth	Wesnoth	1.2.1	All	All	All
Application	Wesnoth	Wesnoth	1.2.2	All	All	All
Application	Wesnoth	Wesnoth	1.2.3	All	All	All
Application	Wesnoth	Wesnoth	1.2.4	All	All	All
Application	Wesnoth	Wesnoth	1.2.5	All	All	All
Application	Wesnoth	Wesnoth	1.2.6	All	All	All
Application	Wesnoth	Wesnoth	1.2.7	All	All	All
Application	Wesnoth	Wesnoth	1.3.1	All	All	All
Application	Wesnoth	Wesnoth	1.3.10	All	All	All
Application	Wesnoth	Wesnoth	1.3.11	All	All	All
Application	Wesnoth	Wesnoth	1.3.2	All	All	All
Application	Wesnoth	Wesnoth	1.3.3	All	All	All
Application	Wesnoth	Wesnoth	1.3.4	All	All	All
Application	Wesnoth	Wesnoth	1.3.5	All	All	All
Application	Wesnoth	Wesnoth	1.3.6	All	All	All
Application	Wesnoth	Wesnoth	1.3.7	All	All	All
Application	Wesnoth	Wesnoth	1.3.8	All	All	All
Application	Wesnoth	Wesnoth	1.3.9	All	All	All

References						
Reference			Source	Link	Tags	
Wesnoth Multiple Vulnerabilities - Advisories - Secunia			SECUNIA	secunia.com	Vendor Advisory	
Wesnoth 1.3.12 - The Battle for Wesnoth Forums			CONFIRM	www.wesnoth.org		
Battle for Wesnoth :: View topic - Wesnoth 1.2.8			CONFIRM	www.wesnoth.org	Patch	
Battle for Wesnoth turn_cmd Remote Denial of Service Vulnerability			BID	www.securityfocus.com	Patch	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			VUPEN	www.vupen.com	Vendor Advisory	
IBM X-Force Exchange			XF	exchange.xforce.ibmcloud.com		
Battle for Wesnoth SourceForge.net			CONFIRM	sourceforge.net	Patch	
CVE Program record			CVE.ORG	www.cve.org	canonical	
NVD vulnerability detail			NVD	nvd.nist.gov	canonical, analysis	

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](#)