



CVE-2005-2842

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

Summary

CVE	CVE-2005-2842
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-09-08 10:03:00 UTC
Updated	2017-09-16 01:29:00 UTC
Description	Buffer overflow in dwr.cs.exe in DameWare Mini Remote Control before 4.9.0 allows remote attackers to execute arbitrary c

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dameware Development	Mini Remote Control Server	4.0	All	All	All
Application	Dameware Development	Mini Remote Control Server	4.1.0.0	All	All	All
Application	Dameware Development	Mini Remote Control Server	4.2.0.0	All	All	All
Application	Dameware Development	Mini Remote Control Server	4.8	All	All	All
Application	Dameware Development	Mini Remote Control Server	4.0	All	All	All
Application	Dameware Development	Mini Remote Control Server	4.1.0.0	All	All	All
Application	Dameware Development	Mini Remote Control Server	4.2.0.0	All	All	All
Application	Dameware Development	Mini Remote Control Server	4.8	All	All	All

References

Reference
DameWare Mini Remote Control Server Pre-Authentication Username Buffer Overflow Vulnerability
Secunia - Advisories - DameWare Mini Remote Control Buffer Overflow Vulnerability
SecurityTracker.com Archives - DameWare Mini Remote Control Buffer Overflow in 'username' Lets Remote Users Execute Arbitrary Code
www.jpno5.com/Releases/Public/Exploits/Dameware%20Mini%20Remote%20Control%2...
Neohapsis Archives - Full Disclosure List - #1074 - [Full-disclosure] Dameware critical hole
Dameware Mini Remote Control 4.0 - Username Stack Buffer Overflow (Metasploit) - Windows remote Exploit

US-CERT Vulnerability Note VU#170905

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

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](#).

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