



CVE-2005-0308

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

Summary

CVE	CVE-2005-0308
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-01-24 05:00:00 UTC
Updated	2017-07-11 01:32:00 UTC
Description	Buffer overflow in the wsprintf function in W32Dasm 8.93 and earlier allows remote attackers to execute arbitrary code via a

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ursoftware	W32dasm	8.94	All	All	All
Application	Ursoftware	W32dasm	8.94	All	All	All

References

Reference	Source
Secunia - Advisories - W32Dasm Import/Export Functions Buffer Overflow	S
SecurityTracker.com Archives - W32Dasm Buffer Overflow in Processing Function Names May Let Remote Users Execute Arbitrary Code	S
IBM X-Force Exchange	X
W32Dasm Buffer Overflow Vulnerability	E
'Local buffer-overflow in W32Dasm 8.93' - MARC	E
CVE Program record	C
NVD vulnerability detail	N

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](#)