



CVE-2006-2875

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2006-2875
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-06-07 00:02:00 UTC
Updated	2018-10-18 16:43:00 UTC
Description	Stack-based buffer overflow in the CL_ParseDownload function of Quake 3 Engine 1.32c and earlier, as used in multiple pr

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Id Software	Quake 3 Engine	All	All	All	All

References

Reference	Source	Link
alugi.altervista.org/adv/q3cbof-adv.txt	MISC	alugi.alte
SecurityFocus	BUGTRAQ	www.seci
SecurityTracker.com Archives - Quake 3 Buffer Overflow in CL_ParseDownload() Permits Remote Code Execution	SECTRACK	securitytr
Secunia - Advisories - Quake3 Engine File Overwrite And Buffer Overflow Vulnerabilities	SECUNIA	secunia.c
Webmail- OVH	VUPEN	www.vup
Quake 3 Engine CL_ParseDownload Remote Buffer Overflow Vulnerability	BID	www.seci
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

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](#)