



CVE-2008-2407

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2008-2407
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-05-23 15:32:00 UTC
Updated	2018-10-11 20:41:00 UTC
Description	Stack-based buffer overflow in AIM.DLL in Cerulean Studios Trillian before 3.1.10.0 allows user-assisted remote attackers t

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ceruleanstudios	Trillian	All	All	All	All

References

Reference

SecurityFocus

IBM X-Force Exchange

Cerulean Studios Trillian Multiple Remote Buffer Overflow Vulnerabilities

Zero Day Initiative

Trillian Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

SecurityTracker.com Archives - Trillian Remote Stack Overflow in AIM.DLL in Parsing HTML Font Parameters Lets Remote Users Execute Ar

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](#)