



# CVE-2008-2409

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

## Summary

<b>CVE</b>	CVE-2008-2409
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2008-05-23 15:32:00 UTC
<b>Updated</b>	2017-08-08 01:31:00 UTC
<b>Description</b>	Stack-based buffer overflow in Cerulean Studios Trillian before 3.1.10.0 allows remote attackers to execute arbitrary code v

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.6351	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.71	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.725	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.73	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74i	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	2.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	2.1	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.5.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.5.1	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.6.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.7.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.9.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.6351	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.71	All	All	All

Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.725	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.73	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74i	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	2.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	2.1	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.5.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.5.1	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.6.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.7.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	3.1.9.0	All	All	All

## References

### Reference

[Cerulean Studios Trillian Multiple Remote Buffer Overflow Vulnerabilities](#)

[Zero Day Initiative](#)

[SecurityTracker.com Archives - Trillian Stack Overflow in Processing X-MMS-IM-FORMAT Header Lets Remote Users Execute Arbitrary Code](#)

[Trillian Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com](#)

[Webmail : Solution de messagerie professionnelle - OVHcloud- OVH](#)

[IBM X-Force Exchange](#)

[20080521 ZDI-08-031: Trillian MSN MIME Header Stack-Based Overflow Vulnerability](#)

[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](#).

