



# CVE-2004-2370

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

## Summary

<b>CVE</b>	CVE-2004-2370
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-12-31 05:00:00 UTC
<b>Updated</b>	2017-07-11 01:31:00 UTC
<b>Description</b>	Stack-based buffer overflow in Trillian 0.71 through 0.74f and Trillian Pro 1.0 through 2.01 allows remote attackers to execu

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.71	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>	0.74b	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74c	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74d	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74e	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74f	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74g	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>	0.74b	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74c	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74d	All	All	All

Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74e	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74f	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian</a>	0.74g	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian Pro</a>	1.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian Pro</a>	2.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian Pro</a>	2.01	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian Pro</a>	1.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian Pro</a>	2.0	All	All	All
Application	<a href="#">Cerulean Studios</a>	<a href="#">Trillian Pro</a>	2.01	All	All	All

## References

Reference	Source	Link
IBM X-Force Exchange	XF	<a href="#">exchange.xforce.ibmcloud.com</a>
e-matters : SECURITY	MISC	<a href="#">security.e-matters.com</a>
Trillian Integer Overflow and Stack Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="#">securitytracker.com</a>
[Full-Disclosure] Advisory 02/2004: Trillian remote overflows	FULLDISC	<a href="#">lists.grok.org.uk</a>
Secunia - Advisories - Trillian Protocol Handling Buffer Overflow Vulnerabilities	SECUNIA	<a href="#">secunia.com</a>
4060	OSVDB	<a href="#">www.osvdb.org</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

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](#)