# CVE-2004-2370

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2004-2370 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2004-12-31 05:00:00 UTC |
| **Updated** | 2017-07-11 01:31:00 UTC |
| **Description** | 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 | Cerulean Studios | Trillian | 0.71 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.725 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.73 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74b | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74c | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74d | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74e | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74f | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74g | All | All | All |
| Application | Cerulean Studios | Trillian | 0.71 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.725 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.73 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74 | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74b | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74c | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74d | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Cerulean Studios | Trillian | 0.74e | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74f | All | All | All |
| Application | Cerulean Studios | Trillian | 0.74g | All | All | All |
| Application | Cerulean Studios | Trillian Pro | 1.0 | All | All | All |
| Application | Cerulean Studios | Trillian Pro | 2.0 | All | All | All |
| Application | Cerulean Studios | Trillian Pro | 2.01 | All | All | All |
| Application | Cerulean Studios | Trillian Pro | 1.0 | All | All | All |
| Application | Cerulean Studios | Trillian Pro | 2.0 | All | All | All |
| Application | Cerulean Studios | Trillian Pro | 2.01 | All | All | All |

## References

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

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.