# CVE-2010-0406

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2010-0406 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2010-05-05 13:22:55 UTC |
| **Updated** | 2026-04-29 01:13:23 UTC |
| **Description** | OpenTTD before 1.0.1 allows remote attackers to cause a denial of service (file-descriptor exhaustion and daemon crash) b |

## Risk And Classification

**Primary CVSS:** v2.0 4 from nvd@nist.gov

AV:N/AC:L/Au:S/C:N/I:N/A:P

**Problem Types:** CWE-399 | n/a

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:S/C:N/I:N/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Openttd | Openttd | 0.1.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Openttd | Openttd | 0.1.2 | All | All | All |
| Application | Openttd | Openttd | 0.1.3 | All | All | All |
| Application | Openttd | Openttd | 0.1.4 | All | All | All |
| Application | Openttd | Openttd | 0.2.0 | All | All | All |
| Application | Openttd | Openttd | 0.2.1 | All | All | All |
| Application | Openttd | Openttd | 0.3.0 | All | All | All |
| Application | Openttd | Openttd | 0.3.1 | All | All | All |
| Application | Openttd | Openttd | 0.3.2 | All | All | All |
| Application | Openttd | Openttd | 0.3.2.1 | All | All | All |
| Application | Openttd | Openttd | 0.3.3 | All | All | All |
| Application | Openttd | Openttd | 0.3.4 | All | All | All |
| Application | Openttd | Openttd | 0.3.5 | All | All | All |
| Application | Openttd | Openttd | 0.3.6 | All | All | All |
| Application | Openttd | Openttd | 0.3.7 | All | All | All |
| Application | Openttd | Openttd | 0.4.0 | All | All | All |
| Application | Openttd | Openttd | 0.4.0.1 | All | All | All |
| Application | Openttd | Openttd | 0.4.5 | All | All | All |
| Application | Openttd | Openttd | 0.4.6 | All | All | All |
| Application | Openttd | Openttd | 0.4.7 | All | All | All |
| Application | Openttd | Openttd | 0.4.8 | All | All | All |
| Application | Openttd | Openttd | 0.4.8 | rc1 | All | All |
| Application | Openttd | Openttd | 0.5.0 | All | All | All |
| Application | Openttd | Openttd | 0.5.0 | rc1 | All | All |
| Application | Openttd | Openttd | 0.5.0 | rc2 | All | All |
| Application | Openttd | Openttd | 0.5.0 | rc3 | All | All |
| Application | Openttd | Openttd | 0.5.0 | rc4 | All | All |
| Application | Openttd | Openttd | 0.5.0 | rc5 | All | All |
| Application | Openttd | Openttd | 0.5.1 | All | All | All |
| Application | Openttd | Openttd | 0.5.1 | rc1 | All | All |
| Application | Openttd | Openttd | 0.5.1 | rc2 | All | All |
| Application | Openttd | Openttd | 0.5.1 | rc3 | All | All |
| Application | Openttd | Openttd | 0.5.2 | All | All | All |
| Application | Openttd | Openttd | 0.5.2 | rc1 | All | All |
| Application | Openttd | Openttd | 0.5.3 | All | All | All |
| Application | Openttd | Openttd | 0.5.3 | rc1 | All | All |
| Application | Openttd | Openttd | 0.5.3 | rc2 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Openttd | Openttd | 0.5.3 | rc3 | All | All |
| Application | Openttd | Openttd | 0.6.0 | All | All | All |
| Application | Openttd | Openttd | 0.6.0 | beta1 | All | All |
| Application | Openttd | Openttd | 0.6.0 | beta2 | All | All |
| Application | Openttd | Openttd | 0.6.0 | beta3 | All | All |
| Application | Openttd | Openttd | 0.6.0 | beta4 | All | All |
| Application | Openttd | Openttd | 0.6.0 | beta5 | All | All |
| Application | Openttd | Openttd | 0.6.0 | rc1 | All | All |
| Application | Openttd | Openttd | 0.6.1 | All | All | All |
| Application | Openttd | Openttd | 0.6.1 | rc1 | All | All |
| Application | Openttd | Openttd | 0.6.1 | rc2 | All | All |
| Application | Openttd | Openttd | 0.6.2 | rc1 | All | All |
| Application | Openttd | Openttd | 0.6.2 | rc2 | All | All |
| Application | Openttd | Openttd | 0.7.4 | All | All | All |
| Application | Openttd | Openttd | All | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| OpenTTD - Security tracker - | af854a3a-2127-422b-91ae-364da2661108 | security.openttd.or |
| OpenTTD Multiple Vulnerabilities - Advisories - Community | af854a3a-2127-422b-91ae-364da2661108 | secunia.com |
| FS#3785 : server leaks file descriptor when client doesn't finish connecting | af854a3a-2127-422b-91ae-364da2661108 | bugs.openttd.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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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**