# CVE-2008-4865

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2008-4865 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2008-11-01 00:00:01 UTC |
| **Updated** | 2026-04-23 00:35:47 UTC |
| **Description** | Untrusted search path vulnerability in valgrind before 3.4.0 allows local users to execute arbitrary programs via a Trojan hor |

## Risk And Classification

**Primary CVSS:** v2.0 7.2 from nvd@nist.gov

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

**Problem Types:** NVD-CWE-Other | n/a

### CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Valgrind | Valgrind | 1.9.6 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Valgrind | Valgrind | 2.0.0 | All | All | All |
| Application | Valgrind | Valgrind | 2.1.0 | All | All | All |
| Application | Valgrind | Valgrind | 2.1.1 | All | All | All |
| Application | Valgrind | Valgrind | 2.2.0 | All | All | All |
| Application | Valgrind | Valgrind | 2.4.1 | All | All | All |
| Application | Valgrind | Valgrind | 2.4.1 | All | powerpc | All |
| Application | Valgrind | Valgrind | 3.0.0 | All | All | All |
| Application | Valgrind | Valgrind | 3.0.1 | All | All | All |
| Application | Valgrind | Valgrind | 3.1.0 | All | All | All |
| Application | Valgrind | Valgrind | 3.1.1 | All | All | All |
| Application | Valgrind | Valgrind | 3.2.0 | All | All | All |
| Application | Valgrind | Valgrind | 3.2.1 | All | All | All |
| Application | Valgrind | Valgrind | 3.2.2 | All | All | All |
| Application | Valgrind | Valgrind | 3.2.3 | All | All | All |
| Application | Valgrind | Valgrind | 3.3.0 | All | All | All |
| Application | Valgrind | Valgrind | 3.3.0 | rc1 | All | All |
| Application | Valgrind | Valgrind | 3.3.0 | rc2 | All | All |
| Application | Valgrind | Valgrind | 3.3.0 | rc3 | All | All |
| Application | Valgrind | Valgrind | 3.3.1 | All | All | All |
| Application | Valgrind | Valgrind | 3.3.1 | rc1 | All | All |
| Application | Valgrind | Valgrind | All | rc1 | All | All |

## Vendor Declared Affected Products

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

## References

| Reference | Source |
|---|---|
| oss-security - Re: CVE request: lynx (old) .mailcap handling flaw | af854a3a-2127-422b-91ae-364da266 |
| oss-security - Re: CVE request: lynx (old) .mailcap handling flaw | af854a3a-2127-422b-91ae-364da266 |
| oss-security - Re: CVE request: lynx (old) .mailcap handling flaw | af854a3a-2127-422b-91ae-364da266 |
| Gentoo Linux Documentation -- Valgrind: Untrusted search path | af854a3a-2127-422b-91ae-364da266 |
| oss-security - Re: CVE request: lynx (old) .mailcap handling flaw | af854a3a-2127-422b-91ae-364da266 |
| [security-announce] SUSE Security Summary Report: SUSE-SR:2009:002 | af854a3a-2127-422b-91ae-364da266 |
| Valgrind, an open-source memory debugger / Thread: [Valgrind-announce] Valgrind-3.4.0 is available | af854a3a-2127-422b-91ae-364da266 |
| SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com | af854a3a-2127-422b-91ae-364da266 |
| CVE Program record | CVE.ORG |

| | |
|---|---|
| CVE Program record | CVE.ORG |
| NVD vulnerability detail | NVD |

## Vendor Comments And Credit

| Organization | Published | Contributor | Statement |
|---|---|---|---|
| Red Hat | 2009-02-05 | Tomas Hoger | Red Hat is aware of this issue and is tracking it via the following bug: https://bugzilla.redhat.com |

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



**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** **status.cve.report**