# CVE-2004-0968

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2004-0968 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2005-02-09 05:00:00 UTC |
| **Updated** | 2025-04-03 01:03:51 UTC |
| **Description** | The catchsegv script in glibc 2.3.2 and earlier allows local users to overwrite files via a symlink attack on temporary files. |

## Risk And Classification

**Primary CVSS:** v2.0 2.1 from nvd@nist.gov

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

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

### CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Gnu | Glibc | 2.0 | All | All | All |
| Application | Gnu | Glibc | 2.0.1 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Gnu | Glibc | 2.0.2 | All | All | All |
| Application | Gnu | Glibc | 2.0.3 | All | All | All |
| Application | Gnu | Glibc | 2.0.4 | All | All | All |
| Application | Gnu | Glibc | 2.0.5 | All | All | All |
| Application | Gnu | Glibc | 2.0.6 | All | All | All |
| Application | Gnu | Glibc | 2.1 | All | All | All |
| Application | Gnu | Glibc | 2.1.1 | All | All | All |
| Application | Gnu | Glibc | 2.1.1.6 | All | All | All |
| Application | Gnu | Glibc | 2.1.2 | All | All | All |
| Application | Gnu | Glibc | 2.1.3 | All | All | All |
| Application | Gnu | Glibc | 2.1.3.10 | All | All | All |
| Application | Gnu | Glibc | 2.1.9 | All | All | All |
| Application | Gnu | Glibc | 2.2 | All | All | All |
| Application | Gnu | Glibc | 2.2.1 | All | All | All |
| Application | Gnu | Glibc | 2.2.2 | All | All | All |
| Application | Gnu | Glibc | 2.2.3 | All | All | All |
| Application | Gnu | Glibc | 2.2.4 | All | All | All |
| Application | Gnu | Glibc | 2.2.5 | All | All | All |
| Application | Gnu | Glibc | 2.3 | All | All | All |
| Application | Gnu | Glibc | 2.3.1 | All | All | All |
| Application | Gnu | Glibc | 2.3.10 | All | All | All |
| Application | Gnu | Glibc | 2.3.2 | All | All | All |
| Application | Gnu | Glibc | 2.3.3 | All | All | All |
| Application | Gnu | Glibc | 2.3.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | advanced_server | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | enterprise_server | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | workstation_server | All |
| Operating System | Redhat | Enterprise Linux Desktop | 3.0 | 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 |
|---|---|---|
| Debian -- Security Information -- DSA-636-1 glibc | af854a3a-2127-422b-91ae-364da2661108 | www.debi |

| | | |
|---|---|---|
| GNU GLibC Insecure Temporary File Creation Vulnerability | af854a3a-2127-422b-91ae-364da2661108 | www.secu |
| 136318 – CAN-2004-0968 temporary file vulnerabilities in catchsegv script | af854a3a-2127-422b-91ae-364da2661108 | bugzilla.re |
| rhn.redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.redh |
| IBM X-Force Exchange | af854a3a-2127-422b-91ae-364da2661108 | exchange |
| Gentoo Linux Documentation -- glibc: Insecure tempfile handling in catchsegv script | af854a3a-2127-422b-91ae-364da2661108 | security.g |
| Repository / Oval Repository | af854a3a-2127-422b-91ae-364da2661108 | oval.cisec |
| www.trustix.org/errata/2004/0050 | af854a3a-2127-422b-91ae-364da2661108 | www.trust |
| usn/usn-4-1 - Ubuntu Linux | af854a3a-2127-422b-91ae-364da2661108 | www.ubur |
| rhn.redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.redh |
| CVE Program record | CVE.ORG | www.cve.( |
| NVD vulnerability detail | NVD | nvd.nist.g |

No vendor comments have been submitted for this CVE.

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**