



# CVE-2005-1123

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

## Summary

|                 |                                                                                                                         |
|-----------------|-------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2005-1123                                                                                                           |
| State           | PUBLISHED                                                                                                               |
| Assigner        | mitre                                                                                                                   |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                            |
| Published       | 2005-05-02 04:00:00 UTC                                                                                                 |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                 |
| Description     | Monkey daemon (monkeyd) before 0.9.1 allows remote attackers to cause a denial of service (memory corruption) via a rec |

## Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

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

|             |                                |                        |       |     |     |     |
|-------------|--------------------------------|------------------------|-------|-----|-----|-----|
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.5.2 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.6.0 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.6.1 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.6.2 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.6.3 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.7.0 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.7.1 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.7.2 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.8.0 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.8.1 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.8.2 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.8.3 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.8.4 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.8.4 | 2   | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 0.8.5 | All | All | All |
| Application | <a href="#">Monkey-project</a> | <a href="#">Monkey</a> | 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                                            |
| Gentoo Bug 87916 - <a href="#">www-servers/monkeyd local DoS+format string bug</a>                              | <a href="#">af854a3a-2127-422b-91ae-364da2661</a> |
| Secunia - Advisories - <a href="#">Monkey HTTP Daemon Denial of Service and Buffer Overflow Vulnerabilities</a> | <a href="#">af854a3a-2127-422b-91ae-364da2661</a> |
| Gentoo Linux Documentation -- <a href="#">monkeyd: Multiple vulnerabilities</a>                                 | <a href="#">af854a3a-2127-422b-91ae-364da2661</a> |
| <a href="#">www.osvdb.org/15512</a>                                                                             | <a href="#">af854a3a-2127-422b-91ae-364da2661</a> |
| CVE Program record                                                                                              | CVE.ORG                                           |
| NVD vulnerability detail                                                                                        | NVD                                               |

No vendor comments have been submitted for this CVE.

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

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)