



# CVE-2006-0381

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

## Summary

|                 |                                                                                                                            |
|-----------------|----------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2006-0381                                                                                                              |
| State           | PUBLISHED                                                                                                                  |
| Assigner        | freebsd                                                                                                                    |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                               |
| Published       | 2006-01-25 22:03:00 UTC                                                                                                    |
| Updated         | 2025-04-03 01:03:51 UTC                                                                                                    |
| Description     | A logic error in the IP fragment cache functionality in pf in FreeBSD 5.3, 5.4, and 6.0, and OpenBSD, when a 'scrub fragme |

## Risk And Classification

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

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

EPSS: 0.051470000 probability, percentile 0.898940000 (date 2026-04-16)

Problem Types: NVD-CWE-Other | 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 |
|------|--------|---------|---------|--------|---------|----------|
|------|--------|---------|---------|--------|---------|----------|

|                  |                         |                         |     |             |     |     |
|------------------|-------------------------|-------------------------|-----|-------------|-----|-----|
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 5.3 | All         | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 5.3 | release     | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 5.3 | releng      | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 5.3 | stable      | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 5.4 | pre-release | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 5.4 | release     | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 5.4 | releng      | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 6.0 | release     | All | All |
| Operating System | <a href="#">Freebsd</a> | <a href="#">Freebsd</a> | 6.0 | stable      | All | All |

| Vendor Declared Affected Products |                    |                     |              |               |
|-----------------------------------|--------------------|---------------------|--------------|---------------|
| Source                            | Vendor             | Product             | Version      | Platforms     |
| CNA                               | <a href="#">Na</a> | <a href="#">N/a</a> | affected n/a | Not specified |

| References                                                                                   |                                                    |
|----------------------------------------------------------------------------------------------|----------------------------------------------------|
| Reference                                                                                    | Source                                             |
| OpenBSD PF IP Fragment Remote Denial Of Service Vulnerability                                | <a href="#">af854a3a-2127-422b-91ae-364da26611</a> |
| <a href="#">www.osvdb.org/22732</a>                                                          | <a href="#">af854a3a-2127-422b-91ae-364da26611</a> |
| IBM X-Force Exchange                                                                         | <a href="#">af854a3a-2127-422b-91ae-364da26611</a> |
| <a href="#">ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2006-004.txt.asc</a>      | <a href="#">af854a3a-2127-422b-91ae-364da26611</a> |
| <a href="#">ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-06:07.pf.asc</a>          | <a href="#">af854a3a-2127-422b-91ae-364da26611</a> |
| SecurityTracker.com Archives - FreeBSD pf(4) Scrub Rule Error Lets Remote Users Deny Service | <a href="#">af854a3a-2127-422b-91ae-364da26611</a> |
| FreeBSD "pf" IP Fragment Denial of Service Vulnerability - Advisories - Secunia              | <a href="#">af854a3a-2127-422b-91ae-364da26611</a> |
| <a href="#">www.openbsd.org/cgi-bin/cvsweb/src/sys/net/pf_norm.c.diff</a>                    | <a href="#">af854a3a-2127-422b-91ae-364da26611</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. |

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)