



# CVE-2001-1342

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                       |
|------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2001-1342                                                                                                         |
| <b>State</b>           | PUBLIC                                                                                                                |
| <b>Assigner</b>        | cve@mitre.org                                                                                                         |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                          |
| <b>Published</b>       | 2001-05-12 04:00:00 UTC                                                                                               |
| <b>Updated</b>         | 2023-11-07 01:55:00 UTC                                                                                               |
| <b>Description</b>     | Apache before 1.3.20 on Windows and OS/2 systems allows remote attackers to cause a denial of service (GPF) via an HT |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor                 | Product                     | Version | Update | Edition | Language |
|-------------|------------------------|-----------------------------|---------|--------|---------|----------|
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.12  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.14  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.15  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.16  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.17  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.18  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.19  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.12  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.14  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.15  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.16  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.17  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.18  | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.19  | All    | win32   | All      |

## References

| Reference | Source | Link |
|-----------|--------|------|
|-----------|--------|------|

|                                                                                                         |         |                                                                       |
|---------------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------------|
| Pony Mail!                                                                                              | MLIST   | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Pony Mail!                                                                                              |         | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| ISS X-Force Database: apache-server-dos (6527): Apache Web Server for Windows and OS2 denial of service | XF      | <a href="http://www.iss.net">www.iss.net</a>                          |
| Pony Mail!                                                                                              | MLIST   | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Pony Mail!                                                                                              | MLIST   | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Pony Mail!                                                                                              |         | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Apache Web Server HTTP Request Denial of Service Vulnerability                                          | BID     | <a href="http://www.securityfocus.com/bid">www.securityf</a>          |
| Pony Mail!                                                                                              |         | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Pony Mail!                                                                                              |         | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| '[Announce] Apache 1.3.20 Released' - MARC                                                              | BUGTRAQ | <a href="http://marc.info">marc.info</a>                              |
| SecurityFocus HOME Mailing List: BugTraq                                                                | BUGTRAQ | <a href="http://online.securityfocus.com/bugtraq">online.security</a> |
| Pony Mail!                                                                                              |         | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Apache Download Mirrors                                                                                 | CONFIRM | <a href="http://bugs.apache.org">bugs.apache.o</a>                    |
| Pony Mail!                                                                                              | MLIST   | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Pony Mail!                                                                                              | MLIST   | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Pony Mail!                                                                                              | MLIST   | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| Pony Mail!                                                                                              |         | <a href="https://lists.apache.org">lists.apache.o</a>                 |
| <a href="http://www.apacheweek.com/issues/01-05-25">www.apacheweek.com/issues/01-05-25</a>              | CONFIRM | <a href="http://www.apache.org">www.apachev</a>                       |
| CVE Program record                                                                                      | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                          |
| NVD vulnerability detail                                                                                | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                        |

| Vendor Comments And Credit |            |             |                                                                                                                                                                     |
|----------------------------|------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Organization               | Published  | Contributor | Statement                                                                                                                                                           |
| Apache                     | 2008-07-02 | Mark J Cox  | Fixed in Apache HTTP Server 1.3.20: <a href="http://httpd.apache.org/security/vulnerabilities_13.html">http://httpd.apache.org/security/vulnerabilities_13.html</a> |

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