



# CVE-2000-0505

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

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2000-0505                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | cve@mitre.org                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2000-05-31 04:00:00 UTC                                                                                                  |
| <b>Updated</b>         | 2023-11-07 01:55:00 UTC                                                                                                  |
| <b>Description</b>     | The Apache 1.3.x HTTP server for Windows platforms allows remote attackers to list directory contents by requesting a UR |

## 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> | 1.3.11  | 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> | 1.3.6   | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.9   | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.11  | 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> | 1.3.6   | All    | win32   | All      |
| Application | <a href="#">Apache</a> | <a href="#">Http Server</a> | 1.3.9   | All    | win32   | All      |
| Application | <a href="#">Ibm</a>    | <a href="#">Http Server</a> | 1.3.3   | All    | win32   | All      |
| Application | <a href="#">Ibm</a>    | <a href="#">Http Server</a> | 1.3.6.2 | All    | win32   | All      |
| Application | <a href="#">Ibm</a>    | <a href="#">Http Server</a> | 1.3.3   | All    | win32   | All      |
| Application | <a href="#">Ibm</a>    | <a href="#">Http Server</a> | 1.3.6.2 | All    | win32   | All      |

## References

| Reference  | Source | Link                                                    | Tags |
|------------|--------|---------------------------------------------------------|------|
| Pony Mail! | MLIST  | <a href="https://lists.apache.org">lists.apache.org</a> |      |
| Pony Mail! |        | <a href="https://lists.apache.org">lists.apache.org</a> |      |

|                                                                |         |                                                                                 |                           |
|----------------------------------------------------------------|---------|---------------------------------------------------------------------------------|---------------------------|
| Pony Mail!                                                     | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| Pony Mail!                                                     | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| Pony Mail!                                                     |         | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| Apache HTTP Server (win32) Root Directory Access Vulnerability | BID     | <a href="https://www.securityfocus.com">www.securityfocus.com</a>               | Exploit, Patch, Vendor Ad |
| Pony Mail!                                                     |         | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| 20000603 Re: IBM HTTP SERVER / APACHE                          | BUGTRAQ | <a href="https://www.securityfocus.com">www.securityfocus.com</a>               | Patch, Vendor Advisory    |
| Pony Mail!                                                     |         | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| Pony Mail!                                                     |         | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| IBM X-Force Exchange                                           | XF      | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |                           |
| Pony Mail!                                                     | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| Pony Mail!                                                     | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| Pony Mail!                                                     | MLIST   | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| Bugtraq                                                        |         | <a href="https://www.securityfocus.com">www.securityfocus.com</a>               |                           |
| Pony Mail!                                                     |         | <a href="https://lists.apache.org">lists.apache.org</a>                         |                           |
| CVE Program record                                             | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                                   | canonical                 |
| NVD vulnerability detail                                       | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>                                 | canonical, analysis       |



## Vendor Comments And Credit

| Organization | Published  | Contributor | Statement                                                                                                                                                           |
|--------------|------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Apache       | 2008-07-02 | Mark J Cox  | Fixed in Apache HTTP Server 1.3.14: <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.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

**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)