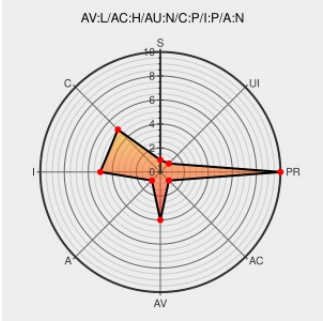
# CVE-2002-1233

Published on: 10/25/2002 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

## CVE-2002-1233

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Http Server from Apache contain the following vulnerability:

A regression error in the Debian distributions of the apache-ssl package (before 1.3.9 on Debian 2.2, and before 1.3.26 on Debian 3.0), for Apache 1.3.27 and earlier, allows local users to read or modify the Apache password file via a symlink attack on temporary files when the administrator runs (1) htpasswd or (2) htdigest, a re-introduction of a vulnerability that was originally identified and addressed by CVE-2001-0131.

CVE-2002-1233 has been assigned by cve@mitre.org to track the vulnerability

## CVSS2 Score: 2.6 - LOW

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | HIGH | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | NONE |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Debian -- Security Information -- DSA-195-1 apache-perl | www.debian.org, Depreciated Link, text/html | DEBIAN DSA-195 |
| Multiple Apache HTDigest and HTPassWD Component Vulnerabilites | cve.report (archive), text/html | BID 5981 |
| ISS X-Force Database: apache-htdigest-tmpfile-race (10413): Apache HTTP Server htdigest temporary file race condition | Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived | XF apache-htdigest-tmpfile-race(10413) |
| Apache HTPasswd Insecure Temporary File Vulnerability | cve.report (archive), text/html | BID 5990 |

| | | |
|---|---|---|
| Debian -- Security Information -- DSA-188-1 apache-ssl | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-188 |
| 'Apache 1.3.26' - MARC | marc.info<br>text/html | BUGTRAQ 20021016 Apache 1.3.26 |
| ISS X-Force Database: apache-htpasswd-tmpfile-race (10412): Apache HTTP Server htpasswd temporary file race condition | web.archive.org<br>text/html<br>Inactive Link Not Archived | XF apache-htpasswd-tmpfile-race(10412) |
| Debian -- Security Information -- DSA-187-1 apache | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-187 |



There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Apache | Http Server | 1.3.17 | All | All | All |
| Application | Apache | Http Server | 1.3.17 | All | win32 | All |
| Application | Apache | Http Server | 1.3.18 | All | All | All |
| Application | Apache | Http Server | 1.3.18 | All | win32 | All |
| Application | Apache | Http Server | 1.3.19 | All | All | All |
| Application | Apache | Http Server | 1.3.19 | All | win32 | All |
| Application | Apache | Http Server | 1.3.20 | All | All | All |
| Application | Apache | Http Server | 1.3.20 | All | win32 | All |
| Application | Apache | Http Server | 1.3.22 | All | All | All |
| Application | Apache | Http Server | 1.3.22 | All | win32 | All |
| Application | Apache | Http Server | 1.3.23 | All | All | All |
| Application | Apache | Http Server | 1.3.23 | All | win32 | All |
| Application | Apache | Http Server | 1.3.24 | All | All | All |
| Application | Apache | Http Server | 1.3.24 | All | win32 | All |
| Application | Apache | Http Server | 1.3.25 | All | All | All |
| Application | Apache | Http Server | 1.3.25 | All | win32 | All |
| Application | Apache | Http Server | 1.3.26 | All | All | All |
| Application | Apache | Http Server | 1.3.26 | All | win32 | All |
| Application | Apache | Http Server | 1.3.27 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Apache | Http Server | 1.3.17 | All | All | All |
| Application | Apache | Http Server | 1.3.17 | All | win32 | All |
| Application | Apache | Http Server | 1.3.18 | All | All | All |
| Application | Apache | Http Server | 1.3.18 | All | win32 | All |
| Application | Apache | Http Server | 1.3.19 | All | All | All |
| Application | Apache | Http Server | 1.3.19 | All | win32 | All |
| Application | Apache | Http Server | 1.3.20 | All | All | All |
| Application | Apache | Http Server | 1.3.20 | All | win32 | All |
| Application | Apache | Http Server | 1.3.22 | All | All | All |
| Application | Apache | Http Server | 1.3.22 | All | win32 | All |
| Application | Apache | Http Server | 1.3.23 | All | All | All |
| Application | Apache | Http Server | 1.3.23 | All | win32 | All |
| Application | Apache | Http Server | 1.3.24 | All | All | All |
| Application | Apache | Http Server | 1.3.24 | All | win32 | All |
| Application | Apache | Http Server | 1.3.25 | All | All | All |
| Application | Apache | Http Server | 1.3.25 | All | win32 | All |
| Application | Apache | Http Server | 1.3.26 | All | All | All |
| Application | Apache | Http Server | 1.3.26 | All | win32 | All |
| Application | Apache | Http Server | 1.3.27 | All | All | All |

cpe:2.3:a:apache:http_server:1.3.17:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.17:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.18:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.18:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.19:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.19:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.20:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.22:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.22:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.23:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.23:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.24:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.24:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.25:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.25:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.26:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.26:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.27:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.17:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.17:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.18:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.18:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.19:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.19:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.20:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.20:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.22:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.22:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.23:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.23:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.24:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.24:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.25:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.25:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.26:*:*:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.26:*:win32:*:*:*:*:*:

cpe:2.3:a:apache:http_server:1.3.27:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**