



# CVE-2002-0840

Published on: 10/11/2002 04:00:00 AM UTC

Last Modified on: 06/06/2021 11:15:00 AM UTC

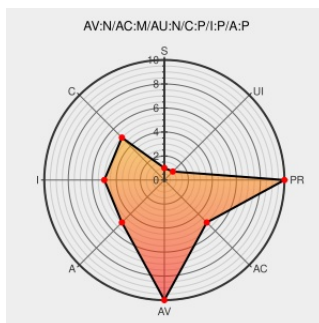
## CVE-2002-0840

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Http Server](#) from [Apache](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the default error page of Apache 2.0 before 2.0.43, and 1.3.x up to 1.3.26, when UseCanonicalName is "Off" and support for wildcard DNS is present, allows remote attackers to execute script as other web page visitors via the Host: header, a different vulnerability than CAN-2002-1157.

CVE-2002-0840 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access Vector

Access Complexity

Authentication

**NETWORK**

**MEDIUM**

**NONE**

Confidentiality Impact

Integrity Impact

Availability Impact

**PARTIAL**

**PARTIAL**

**PARTIAL**

## CVE References

Description

Tags

Link

Pony Mail!

[lists.apache.org](#)  
[text/html](#)

MLIST [httpd-cvs] 20210606 svn commit: r1075470 [1/4] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2020-13938.json security/vulnerabilities\_13.html security/vulnerabilities\_20.html security/vulnerabilities\_22.html security/vulnerabilities\_24.html

Debian --  
Security Information -- DSA-195-1 apache-perl

[www.debian.org](#)  
[Deprecated Link](#)  
[text/html](#)

DEBIAN DSA-195

'[Security Release] Apache HTTP Server 2.0.43' - MARC

[marc.info](#)  
[text/html](#)

CONFIRM [marc.info/?l=apache-httpd-announce&m=103367938230488&w=2](#)

redhat.com | Red Hat Support

[www.redhat.com](#)  
[text/html](#)

REDHAT RHSA-2003:106

|                                                                   |                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| redhat.com   Red Hat Support                                      | <a href="http://www.redhat.com/text/html">www.redhat.com</a><br><a href="#">text/html</a>                                                      |  REDHAT RHSA-2002:222                                                                                                                                                                                                                                                            |
| Apache Server Side Include Cross Site Scripting Vulnerability     | <a href="#">cve.report (archive)</a><br><a href="#">text/html</a>                                                                              |  BID 5847                                                                                                                                                                                                                                                                      |
| Pony Mail!                                                        | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                  |  MLIST [httpd-cvs] 20210603 svn commit: r1075360 [1/3] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html    |
| Pony Mail!                                                        | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                  |  MLIST [httpd-cvs] 20210330 svn commit: r1073140 [1/4] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohtml.py security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html            |
| redhat.com   Red Hat Support                                      | <a href="http://www.redhat.com/text/html">www.redhat.com</a><br><a href="#">text/html</a>                                                      |  REDHAT RHSA-2002:243                                                                                                                                                                                                                                                          |
| Pony Mail!                                                        | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                  |  MLIST [httpd-cvs] 20210330 svn commit: r1073140 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohtml.py security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html            |
| Home - Conectiva                                                  | <a href="http://distro.conectiva.com.br/text/html">distro.conectiva.com.br</a><br><a href="#">text/html</a>                                    |  CONECTIVA CLA-2002:530                                                                                                                                                                                                                                                        |
| Pony Mail!                                                        | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                  |  MLIST [httpd-cvs] 20210330 svn commit: r1073143 [2/3] - in /websites/staging/httpd/trunk/content: ./ security/                                                                                                                                                                |
| redhat.com   Red Hat Support                                      | <a href="http://www.redhat.com/text/html">www.redhat.com</a><br><a href="#">text/html</a>                                                      |  REDHAT RHSA-2002:248                                                                                                                                                                                                                                                        |
| No Description Provided                                           | Vendor Advisory<br><a href="http://www.apacheweek.com/text/html">www.apacheweek.com</a><br><a href="#">text/html</a>                           |  CONFIRM <a href="http://www.apacheweek.com/issues/02-10-04">www.apacheweek.com/issues/02-10-04</a>                                                                                                                                                                          |
| Pony Mail!                                                        | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                  |  MLIST [httpd-cvs] 20190815 svn commit: r1048743 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| Debian -- Security Information -- DSA-188-1 apache-ssl            | <a href="http://www.debian.org/text/html">www.debian.org</a><br><a href="#">Deprecated Link</a><br><a href="#">text/html</a>                   |  DEBIAN DSA-188                                                                                                                                                                                                                                                              |
| IBM X-Force Exchange                                              | <a href="http://exchange.xforce.ibmcloud.com/text/html">exchange.xforce.ibmcloud.com</a><br><a href="#">text/html</a>                          |  XF apache-http-host-xss(10241)                                                                                                                                                                                                                                              |
| '[OpenPKG-SA-2002.009] OpenPKG Security Advisory (apache)' - MARC | <a href="http://marc.info/text/html">marc.info</a><br><a href="#">text/html</a>                                                                |  BUGTRAQ 20021003 [OpenPKG-SA-2002.009] OpenPKG Security Advisory (apache)                                                                                                                                                                                                   |
| CERT/CC Vulnerability Note VU#240329                              | <a href="#">US Government Resource</a><br><a href="http://www.kb.cert.org/text/html">www.kb.cert.org</a><br><a href="#">text/html</a>          |  CERT-VN VU#240329                                                                                                                                                                                                                                                           |
| LinuxSecurity.com: EnGarde: apache vulnerabilities                | <a href="http://www.linuxsecurity.com/text/html">www.linuxsecurity.com</a><br><a href="#">text/html</a>                                        |  ENGARDE ESA-20021007-024                                                                                                                                                                                                                                                    |
| redhat.com   Red Hat Support                                      | <a href="http://www.redhat.com/text/html">www.redhat.com</a><br><a href="#">text/html</a>                                                      |  REDHAT RHSA-2002:244                                                                                                                                                                                                                                                        |
| No Description Provided                                           | <a href="http://www.linux-mandrake.com/Inactive Link">www.linux-mandrake.com</a><br><a href="#">Inactive Link</a> <a href="#">Not Archived</a> |  MANDRAKE MDKSA-2002:068                                                                                                                                                                                                                                                     |
| Pony Mail!                                                        | <a href="#">lists.apache.org</a><br><a href="#">text/html</a>                                                                                  |  MLIST [httpd-cvs] 20040330 svn commit: r1073140 [1/4] - in                                                                                                                                                                                                                  |

|                                                                                        |                                                                                                                 |                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pony Mail!                                                                             | <a href="https://lists.apache.org/text/html">lists.apache.org<br/>text/html</a>                                 | MLIST [httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/                                                                                                                                                        |
| Pony Mail!                                                                             | <a href="https://lists.apache.org/text/html">lists.apache.org<br/>text/html</a>                                 | MLIST [httpd-cvs] 20210606 svn commit: r1075470 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2020-13938.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html  |
| No Description Provided                                                                | <a href="https://www.osvdb.org">www.osvdb.org</a><br><br>Inactive Link Not Archived                             | OSVDB 862                                                                                                                                                                                                                                                                   |
| Neohapsis Archives - Bugtraq - TSLSA-2002-0069-<br>apache - From<br>tsl_at_trustix.com | <a href="https://web.archive.org/text/html">web.archive.org<br/>text/html</a><br><br>Inactive Link Not Archived | BUGTRAQ 20021017 TSLSA-2002-0069-apache                                                                                                                                                                                                                                     |
| No Description Provided                                                                | <a href="https://web.archive.org/text/html">web.archive.org<br/>text/html</a><br><br>Inactive Link Not Archived | VULNWATCH 20021002 Apache 2 Cross-Site Scripting                                                                                                                                                                                                                            |
| redhat.com   Red Hat Support                                                           | <a href="https://www.redhat.com/text/html">www.redhat.com<br/>text/html</a>                                     | REDHAT RHSA-2002:251                                                                                                                                                                                                                                                        |
| Debian -- Security Information -- DSA-187-1 apache                                     | <a href="https://www.debian.org/text/html">www.debian.org<br/>text/html</a><br>Deprecated Link                  | DEBIAN DSA-187                                                                                                                                                                                                                                                              |
| Pony Mail!                                                                             | <a href="https://lists.apache.org/text/html">lists.apache.org<br/>text/html</a>                                 | MLIST [httpd-cvs] 20210330 svn commit: r1073149 [2/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/                                                                                                                                              |
| No Description Provided                                                                | <a href="https://patches.sgi.com">patches.sgi.com</a><br><br>Inactive Link Not Archived                         | SGI 20021105-02-I                                                                                                                                                                                                                                                           |
| Pony Mail!                                                                             | <a href="https://lists.apache.org/text/html">lists.apache.org<br/>text/html</a>                                 | MLIST [httpd-cvs] 20200401 svn commit: r1058586 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| Pony Mail!                                                                             | <a href="https://lists.apache.org/text/html">lists.apache.org<br/>text/html</a>                                 | MLIST [httpd-cvs] 20210330 svn commit: r1073149 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/                                                                                                                                              |
| Pony Mail!                                                                             | <a href="https://lists.apache.org/text/html">lists.apache.org<br/>text/html</a>                                 | MLIST [httpd-cvs] 20200401 svn commit: r1058587 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| SecurityFocus HOME Advisories: Sec. Vulnerability in Apache                            | <a href="https://web.archive.org/text/html">web.archive.org<br/>text/html</a><br><br>Inactive Link Not Archived | HP HPSBUX0210-224                                                                                                                                                                                                                                                           |
| Pony Mail!                                                                             | <a href="https://lists.apache.org/text/html">lists.apache.org<br/>text/html</a>                                 | MLIST [httpd-cvs] 20190815 svn commit: r1048742 [2/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html |
| 'Apache 2 Cross-Site Scripting' - MARC                                                 | <a href="https://marc.info/text/html">marc.info<br/>text/html</a>                                               | BUGTRAQ 20021002 Apache 2 Cross-Site Scripting                                                                                                                                                                                                                              |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no OIDs associated with this CVE

| There are currently no CVEs associated with this CPE |        |             |         |        |         |          |
|------------------------------------------------------|--------|-------------|---------|--------|---------|----------|
|                                                      |        |             |         |        |         |          |
| Known Affected Configurations (CPE V2.3)             |        |             |         |        |         |          |
| Type                                                 | Vendor | Product     | Version | Update | Edition | Language |
| Application                                          | Apache | Http Server | 1.3     | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.1   | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.11  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.12  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.14  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.17  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.18  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.19  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.20  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.22  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.23  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.24  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.25  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.26  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.3   | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.4   | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.6   | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.9   | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0     | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.28  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.32  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.35  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.36  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.37  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.38  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.39  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.40  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.41  | All    | All     | All      |
| Application                                          | Apache | Http Server | 2.0.42  | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3     | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.1   | All    | All     | All      |
| Application                                          | Apache | Http Server | 1.3.11  | All    | All     | All      |

|             |        |                    |          |     |     |     |
|-------------|--------|--------------------|----------|-----|-----|-----|
| Application | Apache | Http Server        | 1.3.12   | All | All | All |
| Application | Apache | Http Server        | 1.3.14   | All | All | All |
| Application | Apache | Http Server        | 1.3.17   | All | All | All |
| Application | Apache | Http Server        | 1.3.18   | All | All | All |
| Application | Apache | Http Server        | 1.3.19   | All | All | All |
| Application | Apache | Http Server        | 1.3.20   | All | All | All |
| Application | Apache | Http Server        | 1.3.22   | All | All | All |
| Application | Apache | Http Server        | 1.3.23   | All | All | All |
| Application | Apache | Http Server        | 1.3.24   | All | All | All |
| Application | Apache | Http Server        | 1.3.25   | All | All | All |
| Application | Apache | Http Server        | 1.3.26   | All | All | All |
| Application | Apache | Http Server        | 1.3.3    | All | All | All |
| Application | Apache | Http Server        | 1.3.4    | All | All | All |
| Application | Apache | Http Server        | 1.3.6    | All | All | All |
| Application | Apache | Http Server        | 1.3.9    | All | All | All |
| Application | Apache | Http Server        | 2.0      | All | All | All |
| Application | Apache | Http Server        | 2.0.28   | All | All | All |
| Application | Apache | Http Server        | 2.0.32   | All | All | All |
| Application | Apache | Http Server        | 2.0.35   | All | All | All |
| Application | Apache | Http Server        | 2.0.36   | All | All | All |
| Application | Apache | Http Server        | 2.0.37   | All | All | All |
| Application | Apache | Http Server        | 2.0.38   | All | All | All |
| Application | Apache | Http Server        | 2.0.39   | All | All | All |
| Application | Apache | Http Server        | 2.0.40   | All | All | All |
| Application | Apache | Http Server        | 2.0.41   | All | All | All |
| Application | Apache | Http Server        | 2.0.42   | All | All | All |
| Application | Oracle | Application Server | 1.0.2    | All | All | All |
| Application | Oracle | Application Server | 1.0.2.1s | All | All | All |
| Application | Oracle | Application Server | 1.0.2.2  | All | All | All |
| Application | Oracle | Application Server | 9.0.2    | All | All | All |
| Application | Oracle | Application Server | 9.0.2    | r2  | All | All |
| Application | Oracle | Application Server | 9.0.2.1  | All | All | All |
| Application | Oracle | Application Server | 1.0.2    | All | All | All |
| Application | Oracle | Application Server | 1.0.2.1s | All | All | All |
| Application | Oracle | Application Server | 1.0.2.2  | All | All | All |
| Application | Oracle | Application Server | 9.0.2    | All | All | All |



|                                            |
|--------------------------------------------|
| cpe:2.3:a:apache:http_server:1.3.19:*****: |
| cpe:2.3:a:apache:http_server:1.3.20:*****: |
| cpe:2.3:a:apache:http_server:1.3.22:*****: |
| cpe:2.3:a:apache:http_server:1.3.23:*****: |
| cpe:2.3:a:apache:http_server:1.3.24:*****: |
| cpe:2.3:a:apache:http_server:1.3.25:*****: |
| cpe:2.3:a:apache:http_server:1.3.26:*****: |
| cpe:2.3:a:apache:http_server:1.3.3:*****:  |
| cpe:2.3:a:apache:http_server:1.3.4:*****:  |
| cpe:2.3:a:apache:http_server:1.3.6:*****:  |
| cpe:2.3:a:apache:http_server:1.3.9:*****:  |
| cpe:2.3:a:apache:http_server:2.0:*****:    |
| cpe:2.3:a:apache:http_server:2.0.28:*****: |
| cpe:2.3:a:apache:http_server:2.0.32:*****: |
| cpe:2.3:a:apache:http_server:2.0.35:*****: |
| cpe:2.3:a:apache:http_server:2.0.36:*****: |
| cpe:2.3:a:apache:http_server:2.0.37:*****: |
| cpe:2.3:a:apache:http_server:2.0.38:*****: |
| cpe:2.3:a:apache:http_server:2.0.39:*****: |
| cpe:2.3:a:apache:http_server:2.0.40:*****: |
| cpe:2.3:a:apache:http_server:2.0.41:*****: |
| cpe:2.3:a:apache:http_server:2.0.42:*****: |
| cpe:2.3:a:apache:http_server:1.3:*****:    |
| cpe:2.3:a:apache:http_server:1.3.1:*****:  |
| cpe:2.3:a:apache:http_server:1.3.11:*****: |
| cpe:2.3:a:apache:http_server:1.3.12:*****: |
| cpe:2.3:a:apache:http_server:1.3.14:*****: |
| cpe:2.3:a:apache:http_server:1.3.17:*****: |
| cpe:2.3:a:apache:http_server:1.3.18:*****: |

|                                                     |
|-----------------------------------------------------|
| cpe:2.3:a:apache:mp_server:1.3.18:*****:            |
| cpe:2.3:a:apache:http_server:1.3.19:*****:          |
| cpe:2.3:a:apache:http_server:1.3.20:*****:          |
| cpe:2.3:a:apache:http_server:1.3.22:*****:          |
| cpe:2.3:a:apache:http_server:1.3.23:*****:          |
| cpe:2.3:a:apache:http_server:1.3.24:*****:          |
| cpe:2.3:a:apache:http_server:1.3.25:*****:          |
| cpe:2.3:a:apache:http_server:1.3.26:*****:          |
| cpe:2.3:a:apache:http_server:1.3.3:*****:           |
| cpe:2.3:a:apache:http_server:1.3.4:*****:           |
| cpe:2.3:a:apache:http_server:1.3.6:*****:           |
| cpe:2.3:a:apache:http_server:1.3.9:*****:           |
| cpe:2.3:a:apache:http_server:2.0:*****:             |
| cpe:2.3:a:apache:http_server:2.0.28:*****:          |
| cpe:2.3:a:apache:http_server:2.0.32:*****:          |
| cpe:2.3:a:apache:http_server:2.0.35:*****:          |
| cpe:2.3:a:apache:http_server:2.0.36:*****:          |
| cpe:2.3:a:apache:http_server:2.0.37:*****:          |
| cpe:2.3:a:apache:http_server:2.0.38:*****:          |
| cpe:2.3:a:apache:http_server:2.0.39:*****:          |
| cpe:2.3:a:apache:http_server:2.0.40:*****:          |
| cpe:2.3:a:apache:http_server:2.0.41:*****:          |
| cpe:2.3:a:apache:http_server:2.0.42:*****:          |
| cpe:2.3:a:oracle:application_server:1.0.2:*****:    |
| cpe:2.3:a:oracle:application_server:1.0.2.1s:*****: |
| cpe:2.3:a:oracle:application_server:1.0.2.2:*****:  |
| cpe:2.3:a:oracle:application_server:9.0.2:*****:    |
| cpe:2.3:a:oracle:application_server:9.0.2:r2:*****: |
| cpe:2.3:a:oracle:application_server:9.0.2.1:*****:  |

|                                                            |
|------------------------------------------------------------|
| cpe:2.3:a:oracle:application_server:1.0.2:~::~::~::~:      |
| cpe:2.3:a:oracle:application_server:1.0.2.1s:~::~::~::~:   |
| cpe:2.3:a:oracle:application_server:1.0.2.2:~::~::~::~:    |
| cpe:2.3:a:oracle:application_server:9.0.2:~::~::~::~:      |
| cpe:2.3:a:oracle:application_server:9.0.2:r2:~::~::~::~:   |
| cpe:2.3:a:oracle:application_server:9.0.2.1:~::~::~::~:    |
| cpe:2.3:a:oracle:database_server:8.1.7:~::~::~::~:         |
| cpe:2.3:a:oracle:database_server:9.2.1:~::~::~::~:         |
| cpe:2.3:a:oracle:database_server:9.2.2:~::~::~::~:         |
| cpe:2.3:a:oracle:database_server:8.1.7:~::~::~::~:         |
| cpe:2.3:a:oracle:database_server:9.2.1:~::~::~::~:         |
| cpe:2.3:a:oracle:database_server:9.2.2:~::~::~::~:         |
| cpe:2.3:a:oracle:oracle8i:8.1.7:~::~::~::~:                |
| cpe:2.3:a:oracle:oracle8i:8.1.7.1:~::~::~::~:              |
| cpe:2.3:a:oracle:oracle8i:8.1.7_0.0_enterprise:~::~::~::~: |
| cpe:2.3:a:oracle:oracle8i:8.1.7_1.0_enterprise:~::~::~::~: |
| cpe:2.3:a:oracle:oracle8i:8.1.7:~::~::~::~:                |
| cpe:2.3:a:oracle:oracle8i:8.1.7.1:~::~::~::~:              |
| cpe:2.3:a:oracle:oracle8i:8.1.7_0.0_enterprise:~::~::~::~: |
| cpe:2.3:a:oracle:oracle8i:8.1.7_1.0_enterprise:~::~::~::~: |
| cpe:2.3:a:oracle:oracle9i:9.0:~::~::~::~:                  |
| cpe:2.3:a:oracle:oracle9i:9.0.1:~::~::~::~:                |
| cpe:2.3:a:oracle:oracle9i:9.0.1.2:~::~::~::~:              |
| cpe:2.3:a:oracle:oracle9i:9.0.1.3:~::~::~::~:              |
| cpe:2.3:a:oracle:oracle9i:9.0.2:~::~::~::~:                |
| cpe:2.3:a:oracle:oracle9i:9.0:~::~::~::~:                  |
| cpe:2.3:a:oracle:oracle9i:9.0.1:~::~::~::~:                |
| cpe:2.3:a:oracle:oracle9i:9.0.1.2:~::~::~::~:              |

cpe:2.3:a:oracle:oracle9i:9.0.1.3:\*\*\*\*\*:

cpe:2.3:a:oracle:oracle9i:9.0.2:\*\*\*\*\*:

[← Previous ID](#)

[Next ID →](#)

© [CVE.report](#) 2023   |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)