# CVE-2004-0885

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2004-0885 |
| **State** | PUBLISHED |
| **Assigner** | mitre |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2004-11-03 05:00:00 UTC |
| **Updated** | 2025-04-03 01:03:51 UTC |
| **Description** | The mod_ssl module in Apache 2.0.35 through 2.0.52, when using the "SSLCipherSuite" directive in directory or location cc |

## Risk And Classification

**Primary CVSS:** v2.0 7.5 from nvd@nist.gov

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

**Problem Types:** NVD-CWE-Other | n/a

### CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| 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 | 2.0.43 | All | All | All |
| Application | Apache | Http Server | 2.0.44 | All | All | All |
| Application | Apache | Http Server | 2.0.45 | All | All | All |
| Application | Apache | Http Server | 2.0.46 | All | All | All |
| Application | Apache | Http Server | 2.0.47 | All | All | All |
| Application | Apache | Http Server | 2.0.48 | All | All | All |
| Application | Apache | Http Server | 2.0.49 | All | All | All |
| Application | Apache | Http Server | 2.0.50 | All | All | All |
| Application | Apache | Http Server | 2.0.51 | All | All | All |
| Application | Apache | Http Server | 2.0.52 | All | All | All |

## Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|---|---|---|---|---|
| CNA | Na | N/a | affected n/a | Not specified |

## References

| Reference | Source | Link |
|---|---|---|
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| rhn.redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.redhat.com |
| rhn.redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.redhat.com |
| usn/usn-177-1 - Ubuntu Linux | af854a3a-2127-422b-91ae-364da2661108 | www.ubuntu.com |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Apache mod_ssl SSLCipherSuite Restriction Bypass Vulnerability | af854a3a-2127-422b-91ae-364da2661108 | www.securityfocus.c |
| www1.itrc.hp.com/service/cki/docDisplay.do | af854a3a-2127-422b-91ae-364da2661108 | www1.itrc.hp.com |
| IBM X-Force Exchange | af854a3a-2127-422b-91ae-364da2661108 | exchange.xforce.ibm |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| #102198: Security Vulnerabilities in the Apache 2 Web Server | af854a3a-2127-422b-91ae-364da2661108 | sunsolve.sun.com |
| httpd 2.0 vulnerabilities - The Apache HTTP Server Project | af854a3a-2127-422b-91ae-364da2661108 | www.apachewatch.c |

| | | |
|---|---|---|
| httpd 2.0 Vulnerabilities - The Apache HTTP Server Project | af854a3a-2127-422b-91ae-364da2661108 | www.apacheweek.c |
| APPLE-SA-2005-08-17 Security Update 2005-007 v1.1 | af854a3a-2127-422b-91ae-364da2661108 | lists.apple.com |
| rhn.redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.redhat.com |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| 1. Overview: | af854a3a-2127-422b-91ae-364da2661108 | support.avaya.com |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Bug 31505 - SSLCipherSuite can be bypassed during renegotiation | af854a3a-2127-422b-91ae-364da2661108 | issues.apache.org |
| '[OpenPKG-SA-2004.044] OpenPKG Security Advisory (modssl)' - MARC | af854a3a-2127-422b-91ae-364da2661108 | marc.info |
| APPLE-SA-2005-08-15 Security Update 2005-007 | af854a3a-2127-422b-91ae-364da2661108 | lists.apple.com |
| Secunia - Advisories - Sun Solaris Multiple Apache2 Vulnerabilities | af854a3a-2127-422b-91ae-364da2661108 | secunia.com |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| redhat.com \| Red Hat Support | af854a3a-2127-422b-91ae-364da2661108 | www.redhat.com |
| Repository / Oval Repository | af854a3a-2127-422b-91ae-364da2661108 | oval.cisecurity.org |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | af854a3a-2127-422b-91ae-364da2661108 | www.vupen.com |
| Pony Mail! | af854a3a-2127-422b-91ae-364da2661108 | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| Pony Mail! | MITRE | lists.apache.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

## Vendor Comments And Credit

| Organization | Published | Contributor | Statement |
|---|---|---|---|
| Apache | 2008-07-02 | Mark J Cox | Fixed in Apache HTTP Server 2.0.53: http://httpd.apache.org/security/vulnerabilities_20.html |

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



**Free CVE JSON API** cve.report/api

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