# CVE-2006-5752

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2006-5752 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2007-06-27 17:30:00 UTC |
| **Updated** | 2023-11-07 01:59:00 UTC |
| **Description** | Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when Ex |

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Apache | Http Server | All | All | All | All |
| Application | Apache | Http Server | 2.2.0 | All | All | All |
| Application | Apache | Http Server | 2.2.3 | All | All | All |
| Application | Apache | Http Server | 2.2.4 | All | All | All |
| Application | Apache | Http Server | 2.2.0 | All | All | All |
| Application | Apache | Http Server | 2.2.3 | All | All | All |
| Application | Apache | Http Server | 2.2.4 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 6.06 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 6.10 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 7.04 | All | All | All |
| Operating System | Fedoraproject | Fedora | 7 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | es | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | ia64 | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | ws | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | as | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | es | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | ws | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Redhat | Enterprise Linux | 4.0 | All | as | All |
| Operating System | Redhat | Enterprise Linux | 4.0 | All | es | All |
| Operating System | Redhat | Enterprise Linux | 4.0 | All | ws | All |
| Operating System | Redhat | Enterprise Linux | 5.0 | All | desktop | All |
| Operating System | Redhat | Enterprise Linux | 5.0 | All | desktop_workstation | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | es | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | ia64 | All |
| Operating System | Redhat | Enterprise Linux | 2.1 | All | ws | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | as | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | es | All |
| Operating System | Redhat | Enterprise Linux | 3.0 | All | ws | All |
| Operating System | Redhat | Enterprise Linux | 4.0 | All | as | All |
| Operating System | Redhat | Enterprise Linux | 4.0 | All | es | All |
| Operating System | Redhat | Enterprise Linux | 4.0 | All | ws | All |
| Operating System | Redhat | Enterprise Linux | 5.0 | All | desktop | All |
| Operating System | Redhat | Enterprise Linux | 5.0 | All | desktop_workstation | All |
| Operating System | Redhat | Enterprise Linux Desktop | 3.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 4.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 3.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 4.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 3.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 4.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 4.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 3.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 4.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 5.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 3.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 4.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 5.0 | All | All | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | ia64 | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | itanium | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | ia64 | All |
| Operating System | Redhat | Linux Advanced Workstation | 2.1 | All | itanium | All |

## References

## References

| Reference |
| --- |
| Red Hat update for httpd - Advisories - Secunia |
| Webmail \| OVH- OVH |
| Pony Mail! |
| Mandriva update for apache - Advisories - Secunia |
| issues.rpath.com/browse/RPL-1500 |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| rhn.redhat.com \| Red Hat Support |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| Pony Mail! |
| IBM HTTP Server "mod_status" Cross-Site Scripting - Advisories - Secunia |
| 2007-0026 |
| rPath update for httpd and mod_ssl - Advisories - Secunia |
| Oracle Critical Patch Update - July 2013 |
| rhn.redhat.com \| Red Hat Support |
| Pony Mail! |
| Fedora update for httpd - Advisories - Secunia |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| rhn.redhat.com \| Red Hat Support |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Security Announcement |
| Pony Mail! |
| [Security-announce] VMSA-2009-0010 VMware Hosted products update libpng and Apache HTTP Server |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Red Hat updates for apache - Advisories - Secunia |

Pony Mail!

Pony Mail!

404 Content not found errors - SunSolve - wikis.sun.com

Pony Mail!

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

rhn.redhat.com | Red Hat Support

Pony Mail!

IBM WebSphere Application Server for z/OS HTTP Server Vulnerabilities - Advisories - Secunia

httpd 1.3 vulnerabilities - The Apache HTTP Server Project

Pony Mail!

IBM X-Force Exchange

245112 – (CVE-2006-5752) CVE-2006-5752 httpd mod_status XSS

Apache Denial of Service and Cross-Site Scripting - Advisories - Secunia

Pony Mail!

Pony Mail!

IBM Search results - United States

Pony Mail!

Apache HTTP Server Mod_Status Cross-Site Scripting Vulnerability

Sun Solaris Apache Cross-Site Scripting and Denial of Service - Advisories - Secunia

Pony Mail!

rhn.redhat.com | Red Hat Support

ASA-2007-353 (RHSA-2007-0557)

httpd 2.2 vulnerabilities - The Apache HTTP Server Project

SecurityFocus

Avaya Products Perl Net::DNS and Apache Vulnerabilities - Advisories - Secunia

Advisories | Mandriva

Gentoo Bug 186219 - www-servers/apache Multiple issues (CVE-2006-{5752}, CVE-2007-{1862,1863,3304,3847,4465})

PK52702: Z/OS IBM HTTP SERVER FOR WEBSPHERE (POWERED BY APACHE) FIX PACK 6.1.0.13

Pony Mail!

Advisories | Mandriva

Advisories | Mandriva

Repository / Oval Repository

#200032: Security Vulnerabilities in the Apache 1.3 and 2.0 Web Server Daemon and "mod_status" Module May Lead to Cross Site Scripting

Trustix Update for Multiple Packages - Advisories - Secunia

Pony Mail!

| |
|---|
| HP-UX update for Apache - Advisories - Secunia |
| Pony Mail! |
| Pony Mail! |
| SecurityTracker.com Archives - Apache mod_status Input Validation Hole Permits Cross-Site Scripting Attacks |
| Interstage HTTP Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com |
| Webmail - OVH |
| 37052 |
| SUSE update for apache2 - Advisories - Secunia |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH |
| HPSBUX02262 SSRT071447 rev. 1 - HP-UX running Apache, Remote Arbitrary Code Execution, Cross Site Scripting (XSS) - c01178795 - HI |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Pony Mail! |
| Gentoo Linux Documentation -- Apache: Multiple vulnerabilities |
| Sun Solaris Apache Cross-Site Scripting and Denial of Service - Advisories - Secunia |
| Ubuntu update for apache - Advisories - Secunia |
| [Apache-SVN] Revision 549159 |
| rhn.redhat.com \| Red Hat Support |
| Apache httpd 2.0 vulnerabilities - The Apache HTTP Server Project |
| This page provides Security Information. : FUJITSU |
| Pony Mail! |
| Gentoo update for apache - Advisories - Secunia |
| Pony Mail! |
| USN-499-1: Apache vulnerabilities \| Ubuntu |
| Pony Mail! |
| [SECURITY] Fedora 7 Update: httpd-2.2.6-1.fc7 |
| Pony Mail! |
| Pony Mail! |
| CVE Program record |
| NVD vulnerability detail |

## Vendor Comments And Credit

| Organization | Published | Contributor | Statement |
|---|---|---|---|
| Apache | 2008-07-02 | Mark J Cox | Fixed in Apache HTTP Server 2.2.6, 2.0.61, and 1.3.39: http://httpd.apache.org/security/vulneral |

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



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