



CVE-2002-0839

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

Summary

CVE	CVE-2002-0839
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2002-10-11 04:00:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	The shared memory scoreboard in the HTTP daemon for Apache 1.3.x before 1.3.27 allows any user running as the Apache user to cause a denial of service (CPU consumption) by sending a series of crafted requests.

Risk And Classification

Primary CVSS: v2.0 7.2 from nvd@nist.gov

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

Problem Types: NVD-CWE-noinfo | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All

Operating System	Debian	Debian Linux	2.2	All	All	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
Pony Mail!				af854a3a-		
www.linux-mandrake.com/en/security/2002/MDKSA-2002-068.php				af854a3a-		
Debian -- Security Information -- DSA-195-1 apache-perl				af854a3a-		
'[Security Release] Apache HTTP Server 2.0.43' - MARC				af854a3a-		
'[security bulletin] HPSBOV02683 SSRT090208 rev.1 - HP Secure Web Server (SWS) for OpenVMS running Ap' - MARC				af854a3a-		
Pony Mail!				af854a3a-		
Home - Conectiva				af854a3a-		
archives.neohapsis.com/archives/vulnwatch/2002-q4/0012.html				af854a3a-		
LinuxSecurity.com: EnGarde: apache vulnerabilities				af854a3a-		
ISS X-Force Database: apache-scorecard-memory-overwrite (10280): Apache HTTP Server shared memory scorecard overwrite				af854a3a-		
www.apacheweek.com/issues/02-10-04				af854a3a-		
patches.sgi.com/support/free/security/advisories/20021105-01-I				af854a3a-		
Pony Mail!				af854a3a-		
'[OpenPKG-SA-2002.009] OpenPKG Security Advisory (apache)' - MARC				af854a3a-		
SecurityFocus HOME Advisories: Sec. Vulnerability in Apache				af854a3a-		
Debian -- Security Information -- DSA-187-1 apache				af854a3a-		
Pony Mail!				af854a3a-		
Apache Web Server Scoreboard Memory Segment Overwriting SIGUSR1 Sending Vulnerability				af854a3a-		
archives.neohapsis.com/archives/bugtraq/2002-10/0195.html				af854a3a-		
Pony Mail!				af854a3a-		
Neohapsis Archives - Bugtraq - TLSA-2002-0069-apache - From tsl_at_trustix.com				af854a3a-		
Debian -- Security Information -- DSA-188-1 apache-ssl				af854a3a-		
Pony Mail!				af854a3a-		
Pony Mail!				MITRE		
Pony Mail!				MITRE		
Pony Mail!				MITRE		
Pony Mail!				MITRE		
Pony Mail!				MITRE		

Pony mail	MITRE
Pony Mail	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 1.3.27: http://httpd.apache.org/security/vulnerabilities_13.html

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

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

Free CVE JSON API [cve.report/api](#)

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