



CVE-2007-0086

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

Summary

CVE	CVE-2007-0086
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-01-05 18:28:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The Apache HTTP Server, when accessed through a TCP connection with a large window size, allows remote attackers to

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

Problem Types: CWE-400 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	-	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	Tags
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	Third Party Advisory, VDB Entry
osvdb.org/33456	af854a3a-2127-422b-91ae-364da2661108	osvdb.org	Broken Link
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	Third Party Advisory, VDB Entry
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	Third Party Advisory, VDB Entry
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.securityfocus.com	Third Party Advisory, VDB Entry
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2007-01-11	Mark J Cox	Red Hat does not consider this issue to be a security vulnerability. The pottential attacker has to

Legacy QID Mappings
900085 CBL-Mariner Linux Security Update for httpd 2.4.46
903071 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (3522)
905908 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (3522-1)