CVE-2004-0493

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2004-0493
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-08-06 04:00:00 UTC
Updated	2023-11-07 01:56:00 UTC
Description	The ap_get_mime_headers_core function in Apache httpd 2.0.49 allows remote attackers to cause a denial of service (mer

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	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	2.0.47	All	All	All
Application	Apache	Http Server	2.0.48	All	All	All
Application	Apache	Http Server	2.0.49	All	All	All
Hardware	Avaya	Converged Communications Server	2.0	All	All	All
Hardware	Avaya	Converged Communications Server	2.0	All	All	All
Hardware	Avaya	S8300	r2.0.0	All	All	All
Hardware	Avaya	S8300	r2.0.0	All	All	All
Hardware	Avaya	S8500	r2.0.0	All	All	All
Hardware	Avaya	S8500	r2.0.0	All	All	All
Hardware	Avaya	S8700	r2.0.0	All	All	All
Hardware	Avaya	S8700	r2.0.0	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Application	Ibm	Http Server	2.0.42	All	All	All

Application	Ibm	Http Server	2.0.42.1	All	All	All
Application	Ibm	Http Server	2.0.42.2	All	All	All
Application	Ibm	Http Server	2.0.47	All	All	All
Application	Ibm	Http Server	2.0.47.1	All	All	All
Application	Ibm	Http Server	2.0.42	All	All	All
Application	Ibm	Http Server	2.0.42.1	All	All	All
Application	Ibm	Http Server	2.0.42.2	All	All	All
Application	Ibm	Http Server	2.0.47	All	All	All
Application	Ibm	Http Server	2.0.47.1	All	All	All
Operating System	Trustix	Secure Linux	1.5	All	All	All
Operating System	Trustix	Secure Linux	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
Operating System	Trustix	Secure Linux	1.5	All	All	All
Operating System	Trustix	Secure Linux	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All

References

Reference	Source	Link
Apache ap_escape_html Memory Allocation Denial Of Service Vulnerability	BID	www.securityfocus.co
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
redhat.com | Red Hat Support	REDHAT	www.redhat.com
'[security bulletin] SSRT4777 HP-UX Apache, PHP remote code execution, Denial of Service' - MARC	HP	marc.info
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Advisories - Mandriva	MANDRAKE	www.mandriva.com
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
httpd 2.0 vulnerabilities - The Apache HTTP Server Project	CONFIRM	www.apacheweek.cor
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org

2004-0039	TRUSTIX	www.trustix.org
DoS in apache httpd 2.0.49, yet still apache much better than windows	MISC	www.guninski.com
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
[Full-Disclosure] DoS in apache httpd 2.0.49, yet still apache much better than windows	FULLDISC	lists.grok.org.uk
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!		lists.apache.org
Repository / Oval Repository	OVAL	oval.cisecurity.org
IBM X-Force Exchange	XF	exchange.xforce.ibmc
Gentoo Linux Documentation -- Apache 2: Remote denial of service attack	GENTOO	security.gentoo.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!		lists.apache.org
Pony Mail!	MLIST	lists.apache.org
Pony Mail!	MLIST	lists.apache.org
'TSSA-2004-012 - apache' - MARC	BUGTRAQ	marc.info
Pony Mail!	MLIST	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 2.0.50: http://httpd.apache.org/security/vulnerabilities_20.html

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