CVE-2004-0809

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2004-0809
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-09-16 04:00:00 UTC
Updated	2023-11-07 01:56:00 UTC
Description	The mod_dav module in Apache 2.0.50 and earlier allows remote attackers to cause a denial of service (child process crash

Risk And Classification

Problem Types: NVD-CWE-noinfo

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	2.0.47	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.47	All	All	All
Application	Apache	Http Server	2.0.50	All	All	All
Operating System	Conectiva	Linux	10.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Conectiva	Linux	10.0	All	All	All
Operating System	Conectiva	Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	3.0	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Gentoo	Linux	1.4	All	All	All
Operating System	Hp	Hp-ux	11.00	All	All	All
Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	11.22	All	All	All
Operating System	Hp	Hp-ux	11.23	All	ia64_64-bit	All
Operating System	Hp	Hp-ux	11.00	All	All	All

Operating System	Hp	Hp-ux	11.11	All	All	All
Operating System	Hp	Hp-ux	11.22	All	All	All
Operating System	Hp	Hp-ux	11.23	All	ia64_64-bit	All
Application	Hp	Secure Web Server For Tru64	4.0_f	All	All	All
Application	Hp	Secure Web Server For Tru64	4.0_g	All	All	All
Application	Hp	Secure Web Server For Tru64	5.0_a	All	All	All
Application	Hp	Secure Web Server For Tru64	5.1	All	All	All
Application	Hp	Secure Web Server For Tru64	5.1_a	All	All	All
Application	Hp	Secure Web Server For Tru64	5.8.1	All	All	All
Application	Hp	Secure Web Server For Tru64	5.8.2	All	All	All
Application	Hp	Secure Web Server For Tru64	5.9.1	All	All	All
Application	Hp	Secure Web Server For Tru64	5.9.2	All	All	All
Application	Hp	Secure Web Server For Tru64	6.3.0	All	All	All
Application	Hp	Secure Web Server For Tru64	4.0_f	All	All	All
Application	Hp	Secure Web Server For Tru64	4.0_g	All	All	All
Application	Hp	Secure Web Server For Tru64	5.0_a	All	All	All
Application	Hp	Secure Web Server For Tru64	5.1	All	All	All
Application	Hp	Secure Web Server For Tru64	5.1_a	All	All	All
Application	Hp	Secure Web Server For Tru64	5.8.1	All	All	All
Application	Hp	Secure Web Server For Tru64	5.8.2	All	All	All
Application	Hp	Secure Web Server For Tru64	5.9.1	All	All	All
Application	Hp	Secure Web Server For Tru64	5.9.2	All	All	All
Application	Hp	Secure Web Server For Tru64	6.3.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.0	All	amd64	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	9.2	All	amd64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All

Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	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	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
Operating System	Turbolinux	Turbolinux Desktop	10.0	All	All	All
Operating System	Turbolinux	Turbolinux Desktop	10.0	All	All	All
Operating System	Turbolinux	Turbolinux Home	All	All	All	All
Operating System	Turbolinux	Turbolinux Home	All	All	All	All
Operating System	Turbolinux	Turbolinux Server	10.0	All	All	All
Operating System	Turbolinux	Turbolinux Server	10.0	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!		lists.apache.org	
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com	
Pony Mail!		lists.apache.org	
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	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Debian -- Security Information -- DSA-558-1 libapache-mod-dav	DEBIAN	www.debian.org	Patch, Vendor
MDKSA-2004:096	MANDRAKE	www.mandrakesecure.net	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
Pony Mail!	MLIST	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	
Pony Mail!	MLIST	lists.apache.org	

Pony Mail!	MLIST	lists.apache.org	
redhat.com | Red Hat Support	REDHAT	www.redhat.com	Vendor Advisc
Pony Mail!		lists.apache.org	
2004-0047	TRUSTIX	www.trustix.org	Exploit, Patch,
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Gentoo Linux Documentation -- Apache 2, mod_dav: Multiple vulnerabilities	GENTOO	www.gentoo.org	Patch, Vendor
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	
404 Not Found	CONFIRM	cvs.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Apache	2008-07-02	Mark J Cox	Fixed in Apache HTTP Server 2.0.51: http://httpd.apache.org/security/vulnerabilities_20.html

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