



CVE-2006-4154

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2006-4154
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-16 19:07:00 UTC
Updated	2017-07-20 01:32:00 UTC
Description	Format string vulnerability in the mod_tcl module 1.0 for Apache 2.x allows context-dependent attackers to execute arbitrary code via crafted input to the %s format string.

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	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.28	beta	win32	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.32	beta	win32	All
Application	Apache	Http Server	2.0.34	beta	win32	All
Application	Apache	Http Server	2.0.35	All	All	All
Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All

Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	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
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.54	All	All	All
Application	Apache	Http Server	2.0.55	All	All	All
Application	Apache	Http Server	2.0.56	All	All	All
Application	Apache	Http Server	2.0.57	All	All	All
Application	Apache	Http Server	2.0.58	All	All	All
Application	Apache	Http Server	2.0.58	All	win32	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.1	All	All	All
Application	Apache	Http Server	2.1.1	All	All	All
Application	Apache	Http Server	2.1.2	All	All	All
Application	Apache	Http Server	2.1.3	All	All	All
Application	Apache	Http Server	2.1.4	All	All	All
Application	Apache	Http Server	2.1.5	All	All	All
Application	Apache	Http Server	2.1.6	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.2	All	windows	All
Application	Apache	Http Server	2.2.3	All	windows	All
Application	Apache	Http Server	2.0	All	All	All
Application	Apache	Http Server	2.0.28	All	All	All
Application	Apache	Http Server	2.0.28	beta	All	All
Application	Apache	Http Server	2.0.28	beta	win32	All
Application	Apache	Http Server	2.0.32	All	All	All
Application	Apache	Http Server	2.0.32	beta	win32	All
Application	Apache	Http Server	2.0.34	beta	win32	All
Application	Apache	Http Server	2.0.35	All	All	All

Application	Apache	Http Server	2.0.36	All	All	All
Application	Apache	Http Server	2.0.37	All	All	All
Application	Apache	Http Server	2.0.38	All	All	All
Application	Apache	Http Server	2.0.39	All	All	All
Application	Apache	Http Server	2.0.40	All	All	All
Application	Apache	Http Server	2.0.41	All	All	All
Application	Apache	Http Server	2.0.42	All	All	All
Application	Apache	Http Server	2.0.43	All	All	All
Application	Apache	Http Server	2.0.44	All	All	All
Application	Apache	Http Server	2.0.45	All	All	All
Application	Apache	Http Server	2.0.46	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
Application	Apache	Http Server	2.0.50	All	All	All
Application	Apache	Http Server	2.0.51	All	All	All
Application	Apache	Http Server	2.0.52	All	All	All
Application	Apache	Http Server	2.0.53	All	All	All
Application	Apache	Http Server	2.0.54	All	All	All
Application	Apache	Http Server	2.0.55	All	All	All
Application	Apache	Http Server	2.0.56	All	All	All
Application	Apache	Http Server	2.0.57	All	All	All
Application	Apache	Http Server	2.0.58	All	All	All
Application	Apache	Http Server	2.0.58	All	win32	All
Application	Apache	Http Server	2.0.9	All	All	All
Application	Apache	Http Server	2.1	All	All	All
Application	Apache	Http Server	2.1.1	All	All	All
Application	Apache	Http Server	2.1.2	All	All	All
Application	Apache	Http Server	2.1.3	All	All	All
Application	Apache	Http Server	2.1.4	All	All	All
Application	Apache	Http Server	2.1.5	All	All	All
Application	Apache	Http Server	2.1.6	All	All	All
Application	Apache	Http Server	2.2	All	All	All
Application	Apache	Http Server	2.2.1	All	All	All
Application	Apache	Http Server	2.2.2	All	windows	All
Application	Apache	Http Server	2.2.2	All	linux	All

Application	Apache	Http Server	2.2.3	All	windows	All
References						
Reference					Source	Li
Gentoo update for mod_tcl - Advisories - Secunia					SECUNIA	se
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					VUPEN	w
Gentoo Linux Documentation -- Apache mod_tcl: Format string vulnerability					GENTOO	se
Public Advisory: 10.13.06 // iDefense Labs					IDEFENSE	la
Apache Mod_TCL Remote Format String Vulnerability					BID	w
Apache HTTP Server mod_tcl Format String Vulnerabilities - Advisories - Secunia					SECUNIA	se
US-CERT Vulnerability Note VU#366020					CERT-VN	w
29536					OSVDB	w
IBM X-Force Exchange					XF	e
Apache mod_tcl Format String Bug in set_var() Function May Let Remote Users Execute Arbitrary Code - SecurityTracker					SECTrack	se
CVE Program record					CVE.ORG	w
NVD vulnerability detail					NVD	nv
No vendor comments have been submitted for this CVE.						
There are currently no legacy QID mappings associated with this CVE.						