



CVE-2009-4491

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2009-4491
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-01-13 20:30:00 UTC
Updated	2023-11-28 17:15:00 UTC
Description	thttpd 2.25b0 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to mod

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Acme	Thttpd	2.25	b	All	All
Application	Acme	Thttpd	2.25	b	All	All

References

Reference	Source	Link	T
www.ush.it/team/ush/hack_httpd_escape/adv.txt	MISC	www.ush.it	E
m-privacy TightGate-Pro Code Execution / Insecure Permissions ≈ Packet Storm		packetstormsecurity.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Full Disclosure: SEC Consult SA-20231122 :: Multiple Vulnerabilities in m-privacy TightGate-Pro		seclists.org	
CVE Program record	CVE.ORG	www.cve.org	cc
NVD vulnerability detail	NVD	nvd.nist.gov	cc

No vendor comments have been submitted for this CVE.

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](#).

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