



# CVE-2013-0348

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2013-0348
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-12-13 18:07:00 UTC
<b>Updated</b>	2023-02-13 04:41:00 UTC
<b>Description</b>	thttpd.c in sthttpd before 2.26.4-r2 and thttpd 2.25b use world-readable permissions for /var/log/thttpd.log, which allows local

## Risk And Classification

**Problem Types:** CWE-264

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Acme</a>	<a href="#">Thttpd</a>	2.25	b	All	All
Application	<a href="#">Acme</a>	<a href="#">Thttpd</a>	2.25	b	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	17	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	18	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	17	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	18	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	All	All	All	All
Operating System	<a href="#">Gentoo</a>	<a href="#">Linux</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.2	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	12.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Opensuse</a>	13.1	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26.1	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26.2	All	All	All

Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26.3	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26.1	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26.2	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	2.26.3	All	All	All
Application	<a href="#">Open Source Development Team</a>	<a href="#">Sthttpd</a>	All	All	All	All

## References

Reference	Source	Link	Tag
458896 – (CVE-2013-0348) <www-servers/thttpd-2.26.4-r2: world-readable logdir (CVE-2013-0348)	CONFIRM	<a href="https://bugs.gentoo.org">bugs.gentoo.org</a>	Pat
924857 – (CVE-2013-0348) CVE-2013-0348 thttpd: World-readable log file	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>	
openSUSE-SU-2013:1862-1: moderate: update for thttpd	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
opensource.dyc.edu/gitweb	MISC	<a href="https://opensource.dyc.edu">opensource.dyc.edu</a>	
openSUSE-SU-2014:0021-1: moderate: update for thttpd	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	
opensource.dyc.edu/gitweb	CONFIRM	<a href="https://opensource.dyc.edu">opensource.dyc.edu</a>	Exp
oss-security - Re: CVE request: sthttpd world-redable logdir	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	car
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	car

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](https://status.cve.report)