

# [VulnWatch] TWiki Security Alert: Arbitrary code execution in session files (CVE-2007-0669)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2007-02/msg00006.html>

---

- *From:* Peter Thoeny <[Peter@xxxxxxxxxxxxxxxxxxxxxxx](mailto:Peter@xxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 08 Feb 2007 09:31:21 -0800
- 

This is a security advisory for TWiki installations:

Local users may cause TWiki to execute arbitrary code by creating CGI session files.

- \* Vulnerable Software Version
- \* Attack Vectors
- \* Impact
- \* Severity Level
- \* MITRE Name for this Vulnerability
- \* Details
- \* Countermeasures
- \* Hotfix for TWiki 4.x
- \* Hotfix for older TWikis using SessionPlugin
- \* Authors and Credits
- \* Action Plan with Timeline
- \* Feedback
- \* External Links

## ----++ Vulnerable Software Version

- \* TWikiRelease04x01x00 -- TWiki-4.1.0.zip
- \* TWikiRelease04x00x05 -- TWiki-4.0.5.zip
- \* TWikiRelease04x00x04 -- TWiki-4.0.4.zip
- \* TWikiRelease04x00x03 -- TWiki-4.0.3.zip
- \* TWikiRelease04x00x02 -- TWiki-4.0.2.zip
- \* TWikiRelease04x00x01 -- TWiki-4.0.1.zip
- \* TWikiRelease04x00x00 -- TWiki-4.0.0.zip
- \* Any previous TWiki version using SessionPlugin [6]

## ----++ Attack Vectors

Write access to global /tmp directory (or CGI session directory, if different). This can be either directly on file level (such as on a shared host), or via an HTTP vulnerability of a third party web application.

#### ---++ Impact

Under the assumption that an intruder has write access to the /tmp directory (or CGI session directory), such as with a vulnerability of another web application running on the same server, it is possible to execute arbitrary Perl code with the privileges of the web server process, such as user "nobody".

#### ---++ Severity Level

The TWiki SecurityTeam [2] triaged this issue as documented in TWikiSecurityAlertProcess [3] and assigned the following severity level:

\* Severity 2 issue: The TWiki installation is compromised

#### ---++ MITRE Name for this Vulnerability

The Common Vulnerabilities and Exposures project has assigned the name CVE-2007-0669 [4] to this vulnerability.

#### ---++ Details

Your site may be vulnerable if:

1. You run one of the vulnerable TWiki versions, and
2. You have *\*not\** reconfigured the CGI session directory `$cfg{Sessions}{Dir}` to a private directory

In particular, disabling the CGI session tracking via `$cfg{UseClientSessions}` is *\*not\** sufficient to protect against this vulnerability, since there is session cleanup code that runs regardless of whether sessions are enabled or not.

#### ---++ Countermeasures

- \* Restrict access to the TWiki server on file level and HTTP.
- \* If on a shared host, move TWiki to a dedicated host.

## [VulnWatch] TWiki Security Alert: Arbitrary code execution in session files (CVE-2007-0669)

- \* Upgrade to TWiki Release 4.1.1 [5] (recommended)
- \* Apply a hotfix indicated below.

NOTE: The hotfix is known to prevent the current attacks, but it might not be a complete fix.

### ---++ Hotfix for TWiki 4.x

In configure, change `$cfg{Sessions}{Dir}` to a private directory (one which is only readable and writable by the user your web server is running as, and is not served as web content to remote users). The recommended fix is to make a `$cfg{DataDir}/session_tmp` directory owned by the user Apache is running as, change its permissions to 0700 (drwx-----), and set `$cfg{Sessions}{Dir}` to that directory.

Upgrading to TWiki 4.1.1 is recommended; the session files are cleaned up by timestamp, i.e. no longer executed. TWiki 4.1.1 will create and use the `/tmp/twiki` directory by default to store the session files.

### ---++ Hotfix for older TWikis using SessionPlugin

This section details the attack vectors, details, and countermeasures for this vulnerability as it applies to the SessionPlugin [6]. This section does not apply to TWiki versions 4.0 and up, which use built-in session tracking.

#### Vulnerable software version

- \* Plugins.SessionPlugin 1.0 --- SessionPlugin.zip (attachment versions 1-5)
- \* Plugins.SessionPlugin 2.0-2.992 -- SessionPlugin.zip (attachment versions 6-8)

#### Attack Vectors

- \* For SessionPlugin 1.000:
  - \* Write access to the `$cfg{DataDir}/.session` directory, which in some cases may be created world-writable for local users.
- \* For SessionPlugin 2.0-2.992:
  - \* Write access to global `/tmp` directory. This can be either directly on file level (such as shared host), or HTTP vulnerability of a third party web application.

#### Countermeasures

- \* For SessionPlugin 1.000 (attachment versions 1-5 from the SessionPlugin topic):
  - \* Ensure that the \$cfg{DataDir}/.session directory exists, is owned by the user Apache is running as, and has 0700 permissions (drwx-----).
- \* For SessionPlugin 2.9 (attachment versions 6-8 from the SessionPlugin topic):
  - \* Upgrade to Plugins.SessionPlugin 2.992 (attachment version 9 from the SessionPlugin topic).

#### ----++ Authors and Credits

- \* Credit to Andrew Moise for disclosing the issue to the twiki-security mailing list
- \* Kenneth Lavrsen and Andrew Moise for creating the hotfix
- \* Andrew Moise and Peter Thoeny for creating the advisory

#### ----++ Action Plan with Timeline

- \* 2007-01-28: User discloses vulnerability to twiki-security
- \* 2007-01-29: Developer verifies issue
- \* 2007-01-31: Developer fixes code and creates hotfix
- \* 2007-02-05: Security team creates advisory
- \* 2007-02-06: Send alert to TWiki-Announce mailing list and TWiki-Dev mailing list
- \* 2007-02-08: Publish advisory in Codev web and update all related topics
- \* 2007-02-08: Issue a public security advisory

#### ----++ Feedback

Please provide feedback at the security alert topic [1],  
<http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2007-0669>

#### ----++ External Links

- [1]: <http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2007-0669>
- [2]: <http://twiki.org/cgi-bin/view/Codev/SecurityTeam>
- [3]: <http://twiki.org/cgi-bin/view/Codev/TWikiSecurityAlertProcess>

[VulnWatch] TWiki Security Alert: Arbitrary code execution in session files (CVE-2007-0669)

[4]: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0669>

[5]: <http://twiki.org/cgi-bin/view/Codev/DownloadTWiki>

[6]: <http://twiki.org/cgi-bin/view/Plugins/SessionPlugin>

-- Contributors: Andrew Moise, Kenneth Lavrsen, Peter Thoeny - 08 Feb 2007

--

\* Peter Thoeny Peter AT StructuredWikis DOT com

\* <http://StructuredWikis.com> - bringing wikis to the workplace

\* <http://TWiki.org> - is your team already TWiki enabled?

\* Knowledge cannot be managed, it can be discovered and shared

\* This e-mail is: ( ) private ( ) ask first (x) public