

# [UNIX] TWiki Arbitrary Code Execution in Session Files

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00027.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxxx)>
  - *Date:* 11 Feb 2007 19:08:35 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

TWiki Arbitrary Code Execution in Session Files

---

## SUMMARY

" <<http://twiki.org/>> TWiki – flexible, powerful, and easy to use enterprise collaboration platform and knowledge management system." Local users may cause TWiki to execute arbitrary code by creating CGI session files.

## DETAILS

Vulnerable Systems:

- \* TWiki version 4.1.0
- \* TWiki version 4.0.0 up to version 4.0.5
- \* Any previous TWiki version using SessionPlugin

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.

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

## [UNIX] TWiki Arbitrary Code Execution in Session Files

execute arbitrary Perl code with the privileges of the web server process, such as user "nobody".

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

CVE Information:

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

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.

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

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.

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)

## [UNIX] TWiki Arbitrary Code Execution in Session Files

### 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).

### Disclosure 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

### External Links:

- [1]: <<http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2007-0669>>  
<http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2007-0669>
- [2]: <<http://twiki.org/cgi-bin/view/Codev/SecurityTeam>>  
<http://twiki.org/cgi-bin/view/Codev/SecurityTeam>
- [3]: <<http://twiki.org/cgi-bin/view/Codev/TWikiSecurityAlertProcess>>  
<http://twiki.org/cgi-bin/view/Codev/TWikiSecurityAlertProcess>
- [4]: <<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0669>>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0669>
- [5]: <<http://twiki.org/cgi-bin/view/Codev/DownloadTWiki>>  
<http://twiki.org/cgi-bin/view/Codev/DownloadTWiki>
- [6]: <<http://twiki.org/cgi-bin/view/Plugins/SessionPlugin>>  
<http://twiki.org/cgi-bin/view/Plugins/SessionPlugin>

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:Peter@xxxxxxxxxxxxxxxxxxxxxx>>  
Peter Thoeny.

The original article can be found at:

<<http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2007-0669>>  
<http://twiki.org/cgi-bin/view/Codev/SecurityAlert-CVE-2007-0669>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.