

[UNIX] TWiki Arbitrary Code Execution in Session Files

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

- *From:* SecuriTeam <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.