

# [VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-07/msg00016.html>

---

- *From:* Peter Thoeny <[Peter@xxxxxxxxxxxxxxxxxxxxxx](mailto:Peter@xxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Thu, 27 Jul 2006 22:35:01 -0700
- 

This is a security advisory for TWiki installations:

Unauthorized user may execute arbitrary commands in case the TWiki configure script is not access restricted.

TWiki is an enterprise collaboration platform. It is a Structured Wiki, typically used to run a project development space, a document management system, a knowledge base, or any other groupware tool. Users without programming skills can create web applications. Developers can extend the functionality of TWiki with Plugins.

Table of Contents:

- \* Vulnerable Software Version
- \* Attack Vectors
- \* Impact
- \* Severity Level
- \* MITRE Name for this Vulnerability
- \* Details
- \* Countermeasures
- \* Hotfixes
- \* Authors and Credits
- \* Action Plan with Timeline
- \* Feedback
- \* External Links

---++ Vulnerable Software Version

- \* TWikiRelease04x00x04 -- TWiki-4.0.4.zip
- \* TWikiRelease04x00x03 -- TWiki-4.0.3.zip
- \* TWikiRelease04x00x02 -- TWiki-4.0.2.zip

## [VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)

- \* TWikiRelease04x00x01 -- TWiki-4.0.1.zip
- \* TWikiRelease04x00x00 -- TWiki-4.0.0.zip

### ----++ Attack Vectors

Supply a specially crafted HTTP POST request on the TWiki configure script.

### ----++ Impact

An intruder is able to execute arbitrary shell commands with the privileges of the web server process, such as user nobody. Properly configured TWiki sites with authenticated configure script are not affected.

### ----++ Severity Level

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

- \* Severity 1 issue: The web server can be compromised

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

The Common Vulnerabilities and Exposures project has assigned the name CVE-2006-3819 [4] to this vulnerability.

### ----++ Details

All TWiki 4.0.x releases have an unsafe eval in twiki/bin/configure which can be exploited to evaluate arbitrary Perl code and run arbitrary commands as the httpd user.

The exploit requires creating a special form to submit a crafted TYPEOF parameter to the configure script. Example:

```
<form method="post" action="/twiki/bin/configure" />
<input type="hidden" name="action" value="update" />
<input type="text"
name="TYPEOF:);system('/bin/touch /tmp/whoops');my @a=(
value="anything" />
<input type="submit" name="submit" value="Submit" />
</form>
```

## [VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)

This results in the following code being evaluated:

```
$def = defined( $TWiki::cfg);  
system('/usr/bin/touch /tmp/whoops');my @a=( );
```

As expected, the file /tmp/whoops appears on the server. The last bit simply avoids a syntax error.

### ---++ Countermeasures

- \* Restrict access to the TWiki configure script.
  - \* Apply the hotfix indicated below.
- NOTE: The hotfix is known to prevent the current attacks, but it might not be a complete fix

### ---++ Hotfixes

This section describes how to protect a TWiki installation on two levels.

- \* Level 1: Restrict access to the configure script
- \* Level 2: Hotfix download for TWiki 4.0.4

#### ---+++ Level 1: Restrict access to the configure script

The configure script should be protected from general access. It is a tool designed for administrators only and should be restricted to invocation by them only. This is typically done by using the basic Apache authentication. The configure script cannot save any settings once the password has been saved for the first time, but the script could still be vulnerable to specially crafted field values. In addition, the script reveals many details about the webserver that should not be made public.

In order to protect TWiki's configure script you can choose between two methods:

- \* Limit access to specific local IP addresses.
- \* Limit access to a few administrator users.

The access restriction can be done using Apache http.conf files or .htaccess files.

Protection of configure using Apache config files:

The example below shows the part of an example Apache config file that configures the TWiki =bin= directory.

## [VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)

```
<Directory "/home/httpd/twiki/bin">
AllowOverride None
Order Allow,Deny
Allow from all
Deny from env=anonymous_spider

Options ExecCGI FollowSymLinks
SetHandler cgi-script

# Password file for TWiki users
AuthUserFile /var/www/twiki/data/.htpasswd
AuthName 'Enter your WikiName: (First name and last name,
no space, no dots, capitalized, e.g. JohnSmith).'
AuthType Basic

# File to return on access control error (e.g. wrong
# password). By convention this is the TWikiRegistration
# page, that allows users to register with the TWiki.
# Apache requires this to be a *local* path.
ErrorDocument 401 /twiki/bin/view/TWiki/TWikiRegistration

# Limit access to configure to specific IP addresses and
# or users. Make sure configure is not open to the general
# public. The configure script is designed for
# administrators only. The script itself and the
# information it reveals can be abused by attackers if not
# properly protected against public access. Replace
# JohnDoe with the login name of the administrator.
<FilesMatch "^configure.*">
SetHandler cgi-script
Order Deny,Allow
Deny from all
Allow from 127.0.0.1, 192.168.1.10
Require user JohnDoe
Satisfy Any
</FilesMatch>

# When using Apache type login the following defines the
# TWiki scripts that makes Apache ask the browser to
# authenticate. It is correct that scripts such as view
# are not authenticated. (un-comment to activate)
#<FilesMatch
"(attach|edit|manage|rename|save|upload|mail|login|.*auth).*">
# require valid-user
#</FilesMatch>

</Directory>
```

The parts that protect the configure script are:

\* The AuthUserFile, AuthName and AuthType defined the

type of authentication and the password file location.

This is required to limit the access to specific users.

\* In the FilesMatch section the "Require user JohnDoe" defined who has access to the configure script.

\* In the FilesMatch section the "Allow from 127.0.0.1, 192.168.1.10" limits access to these two IP addresses.

Note that the first is localhost.

\* In the FilesMatch section the "Satisfy Any" means that either the login name or the IP address must be valid.

If you only setup one of the protections you can remove this. If you want IP address match and login to be required change this to "Satisfy All"

Above Apache config example is taken from file twiki\_httpd\_conf.txt, located in the root of your TWiki installation after upgrading it to TWiki-4.0.4 Hotfix 2 [6]. The accumulated Hotfix 2 for TWiki-4.0.4 [5] can be downloaded from

<http://twiki.org/cgi-bin/view/Codev/HotFix04x00x04x02>

If you configure Apache via .htaccess files:

If you configure your Apache via .htaccess files the protection method is identical to the method with config files, with these exceptions:

- \* A .htaccess file is put in the bin directory
- \* The same <FilesMatch "^configure.\*"> section is placed in the .htaccess file
- \* The <Directory> </Directory> section is not needed.

An example .htaccess.txt file is located in the bin of your TWiki installation after upgrading it to TWiki-4.0.4 Hotfix 2 [6]. The accumulated Hotfix 2 for TWiki-4.0.4 [5] can be downloaded from

<http://twiki.org/cgi-bin/view/Codev/HotFix04x00x04x02>

Apache Config Generator:

You can quickly create a complete Apache config file, tailored to your installation, at TWiki:TWiki.ApacheConfigGenerator [7]. It protects also the configure script, based on your preference.

---+++ Level 2: Hotfix download for TWiki 4.0.4

An accumulated Hotfix 2 for TWiki-4.0.4 is available for download. It contains an improved version of the configure script, fixing the known vulnerability. It is available at <http://twiki.org/cgi-bin/view/Codev/HotFix04x00x04x02>

## [VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)

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

- \* Credit to TWiki:Main.BenWheeler for disclosing the issue to the twiki-security mailing list
- \* TWiki:Main.CrawfordCurrie for creating a fix
- \* TWiki:Main.KennethLavrsen for creating a hotfix for TWiki release 4.0.4
- \* TWiki:Main.PeterThoeny and TWiki:Main.KennethLavrsen for creating the advisory

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

- \* 2006-07-21: User discloses vulnerability to twiki-security
- \* 2006-07-22: Developer verifies issue
- \* 2006-07-23: Developer creates fix
- \* 2006-07-25: Developer creates hotfix
- \* 2006-07-25: Security team creates advisory
- \* 2006-07-26: Send alert to twiki-announce mailing list and twiki-dev mailing list
- \* 2006-07-26: Publish advisory on TWiki.org
- \* 2006-07-28: Issue a public security advisory (pending)

### ----++ Feedback

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

### ----++ External Links

- [1]: <http://twiki.org/cgi-bin/view/Codev/SecurityAlertCmdExecWithConfigure>
- [2]: <http://twiki.org/cgi-bin/view/Codev/SecurityTeam>
- [3]: <http://twiki.org/cgi-bin/view/Codev/TWikiSecurityAlertProcess>
- [4]: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3819>
- [5]: <http://twiki.org/cgi-bin/view/Codev/TWikiRelease04x00x04>
- [6]: <http://twiki.org/cgi-bin/view/Codev/HotFix04x00x04x02>
- [7]: <http://twiki.org/cgi-bin/view/TWiki/ApacheConfigGenerator>

-- Contributors: KennethLavrsen, CrawfordCurrie, PeterThoeny  
- 27 Jul 2006

--

- \* Peter Thoeny Peter@xxxxxxxxxxxxxxxxxxxxxx
- \* <http://StructuredWikis.com> - bringing wikis to the workplace
- \* <http://TWiki.org> - is your team already TWiki enabled?

[VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)

[VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)

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

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

[VulnWatch] TWiki Security Alert: Configure Script Allows Arbitrary Shell Command Execution (CVE-2006-3819)