

[VulnWatch] TWiki Security Advisory: Privilege elevation with crafted registration form (CVE-2006-2942)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-06/msg00004.html>

- *From:* Peter Thoeny <Peter@xxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 16 Jun 2006 19:59:27 -0700
-

This is a security advisory for TWiki 4.0 installations:
Unauthorized user may gain TWiki admin group privileges with a custom registration form.

TOC:

- * Vulnerable Software Version
- * Attack Vectors
- * Impact
- * Severity Level
- * MITRE Name for this Vulnerability
- * Details
- * Countermeasures
- * Authors and Credits
- * Hotfix for TWiki 4.0.0, 4.0.1 and TWiki 4.0.2
- * Feedback
- * External Links

---++ Vulnerable Software Version

- * TWikiRelease04x00x02 -- TWiki-4.0.2.zip
- * TWikiRelease04x00x01 -- TWiki-4.0.1.zip
- * TWikiRelease04x00x00 -- TWiki-4.0.0.zip

---++ Attack Vectors

TWiki's registration process can be invoked with a crafted version of the original HTML form in which the action attribute of the form element has been modified to point to the Sandbox web instead of the user web. In this case, TWiki's validation fails to correctly check whether the wikiname of the user has already been registered. The wikiname's user topic is looked for in the web as given by the action attribute instead of the user web.

[VulnWatch] TWiki Security Advisory: Privilege elevation with crafted registration form (CVE-2006-2942)

An attacker can use this to register with his own login name, stealing a wiki name which has already been registered.

---++ Impact

In a TWiki where login names are allowed, an attacker can snatch the WikiName of a known member of the TWikiAdminGroup and associate it with his own login name. After login, the attacker can act with the privileges of TWikiAdminGroup, i.e. unlimited access with regard to the TWiki topics.

Even if there is no known threat to TWiki 4 installations with {MapUserToWikiName} flag unchecked in configure, it is recommended that all TWiki 4 installations have this hotfix installed so that the registration code is clean and safe from further exploits.

---++ Severity Level

The TWiki SecurityTeam [3] triaged this issue as documented in TWiki Security Alert Process [2] 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-2006-2942 to this vulnerability [4].

---++ Details

How to reproduce:

Take a copy of the HTML version of TWiki.TWikiRegistration, and change the action parameter in the form from ...bin/register/Main/WebHome to ...bin/register/Sandbox/WebHome. Using the modified form, register with the WikiName of a member of the TWikiAdminGroup, but provide the attacker's login name.

The registration "succeeds" to a sufficient extent: TWiki creates a new "personal homepage" for the attacker in the Sandbox web, but this doesn't matter. TWikiUsers is changed, and is now showing the attacker's login name next to the administrator's WikiName.

[VulnWatch] TWiki Security Advisory: Privilege elevation with crafted registration form (CVE-2006-2942)

Why this succeeds:

During the registration process, the code "verifies" the form data, and during this verification process tries to check whether the user home page exists. However, when doing so, it does not refer explicitly to the users web. The offending line is:

```
if($session->{store}->topicExists( $data->{webName},  
$data->{WikiName} )) {
```

In this line, and again when trying to create the user home page, TWiki should under no circumstances rely on the data provided by the query, but always use `=$TWiki::cfg{UsersWebName}=`.

----++ Countermeasures

- * Apply hotfix
- * Upgrade to TWiki 4.0.3 (to be released in a few days)

----++ Authors and Credits

- * Credit to TWiki:Main.HaraldJoerg for disclosing the issue to the twiki-security mailing list
- * TWiki:Main.HaraldJoerg for providing a fix and for fixing the code for TWiki 4.0.3
- * TWiki:Main.KennethLavrsen for creating a hotfix
- * TWiki:Main.PeterThoeny and TWiki:Main.KennethLavrsen for creating the advisory

----++ Hotfix for TWiki 4.0.0, 4.0.1 and TWiki 4.0.2

A hotfix for all released versions of TWiki 4.0.X has been attached to the security alert topic,
<http://twiki.org/cgi-bin/view/Codev/SecurityAlertTWiki4PrivilegeElevation>

The hotfix updates one single file: `lib/TWiki/UI/Register.pm`. The hotfix is provided in two formats: Patch file or a new replacement `Register.pm` file. The patch file is the best option if you have altered the TWiki code yourself. The replacement file is the simpler choice for most. All you need to do is replace the file provided.

- * CVE-2006-2942-hotfix-4.0.0-4.0.2.diff – Patch file for `lib/TWiki/UI/Register.pm`. This patch file is compatible with 4.0.0, 4.0.1 and 4.0.2. Change directory to `lib/TWiki/UI`, copy the patch file to this directory and apply the patch with the command: `patch < CVE-2006-2942-hotfix-4.0.0-4.0.2.diff`.

[VulnWatch] TWiki Security Advisory: Privilege elevation with crafted registration form (CVE-2006-2942)

You can delete the patch file afterwards.

- * CVE-2006-2942-Register.pm-4.0.0-4.0.1.zip – Replacement file lib/TWiki/UI/Register.pm for TWiki 4.0.0 and TWiki 4.0.1
- * CVE-2006-2942-Register.pm-4.0.2.zip – Replacement file lib/TWiki/UI/Register.pm for TWiki 4.0.2

---++ Feedback

Please provide feedback at

<http://twiki.org/cgi-bin/view/Codev/SecurityAlertTWiki4PrivilegeElevation>

---++ External Links

[1]:

<http://twiki.org/cgi-bin/view/Codev/SecurityAlertTWiki4PrivilegeElevation>

[2]: <http://twiki.org/cgi-bin/view/Codev/TWikiSecurityAlertProcess>

[3]: <http://twiki.org/cgi-bin/view/Codev/SecurityTeam>

[4]: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2942>

— Contributors: Main.HaraldJoerg, Main.CrawfordCurrie, Main.PeterThoeny, Main.KennethLavrson – 16 Jun 2006

—

* Peter Thoeny Peter@xxxxxxxxxxxxxxxxxxxxxx

* <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