

[UNIX] Gaim Arbitrary Email Access

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0064.html>

From: support@securiteam.com

Date: 05/14/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 14 May 2002 08:24:16 +0200 (CEST)

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.

Gaim Arbitrary Email Access

SUMMARY

<<http://sourceforge.net/projects/gaim/>> Gaim is an all-in-one IM client that resembles AIM. Gaim lets you use AIM, ICQ, Yahoo, MSN, IRC, Jabber, Napster, Zephyr, and Gadu-Gadu, all at once. Gaim is NOT endorsed by or affiliated with AOL, Yahoo, MSN, or Napster. A security vulnerability has been found in the way the product uses the "/tmp" directory, that would allow local attackers to gain a valid Session ID, and effectively be able to login into other people's account without knowing their username or password.

DETAILS

Vulnerable systems:

Gaim version 0.57 and prior

Immune systems:

Gaim version 0.58

Gaim uses /tmp as a dumping ground for many temporary files. Here is what the problem is:

1) Gaim starts up and checks your hotmail email (if this option is enabled in your Gaim setup)

Securiteam: [UNIX] Gaim Arbitrary Email Access

2) It will create two files in /tmp. These files are named:
file<someRandomletters> – e.g. fileFH9e0w or file984345

3) These files have permission:
4 -rw-rw-r-- 1 smackenz smackenz 978 May 12 03:01 /tmp/file984345
(Where smackenz is the Gaim user).

** As you can see they are readable by anyone **

If we then close Gaim (or leave it open), and go into /tmp as a different user (or even from a different computer), and use a web browser (for example) Konqueror to open one of the two files, it takes you straight to the Gaim user's hotmail inbox, where you will have full access.

IMPORTANT This only works whilst the other user is running Gaim, or only for a minute or so after the user closes Gaim – probably due to the fact that after Gaim is closed a session ID from hotmail will change, therefore making your session ID in the 'stolen' file incorrect.

```
#more /tmp/file*
< skipped for easy reading>...
<input type="hidden" name="auth"
value="2AAAAAAAADfFg7dCWdlevXUGqgbzqmlMIWYjtXUaSbSpr*zqdYziwIhw$$">
<input type="hidden" name="creds"
value="aec291f9a02b4837de38eb661dbf9847">
```

Solution:

The product has been patched, the latest version is available via CVS, and is fixed as of version 0.58. It is best to fix this problem until 0.58 comes out on high user systems running Gaim – get the latest CVS.

ADDITIONAL INFORMATION

The information has been provided by <mailto:smackenz@sdf.lonestar.org>
Scott Mackenzie.

=====

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.

Securiteam: [UNIX] Gaim Arbitrary Email Access

- ***Previous message:*** support@securiteam.com: "[\[NEWS\] MSCAPI CSP Install Wizard Incorrect Behavior Pose a Security Threat](#)"
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)