

[UNIX] Tripwire Format String Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-06/0011.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/03/04

To: list@securiteam.com

Date: 3 Jun 2004 20:01:43 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Tripwire Format String Vulnerability

SUMMARY

<<http://www.Tripwire.org>> Tripwire(tm) is a "Security, Intrusion Detection, Damage Assessment and Recovery, Forensics software". A vulnerability in the product allows a user on the local machine under certain circumstances to execute arbitrary code with the rights of the user running the program (typically root).

DETAILS

Vulnerable Systems:

- * Tripwire commercial versions prior and including 2.4
- * Tripwire open source versions prior and including 2.3.1

A format string vulnerability exists when tripwire generates an email report (i.e. 'tripwire -m c -M'). Each line of the report is passed to an fprintf() function in pipedmailmessage.cpp in the following manner:

```
fprintf(mpFile, s.c_str() );
```

If a local user were to create a file with a carefully crafted filename on the local system, that filename may be included in the report and passed to fprintf() (albeit from the heap.) No exploit is known at this time, but the author of this advisory believes this vulnerability could be

Securiteam: [UNIX] Tripwire Format String Vulnerability

exploitable.

Tripwire Inc. has been notified and has implemented a fix.

Impact:

This vulnerability allows an attacker to execute arbitrary code with the rights of the user running the file check, which is typically root. The vulnerability exists only when tripwire is used to generate an email report. Users who do not generate an email report are not affected by this vulnerability.

Workaround:

Disable email reporting. All users are advised to upgrade to a version that is not vulnerable.

Patch:

If you are using Open Source Tripwire(tm) version 2.3.1, the following patch will fix this particular issue:

Index: src/tripwire/pipedmailmessage.cpp

```
=====
retrieving revision 1.1
retrieving revision 1.2
diff -u -r1.1 -r1.2
--- src/tripwire/pipedmailmessage.cpp 21 Jan 2001 00:46:48 -0000 1.1
+++ src/tripwire/pipedmailmessage.cpp 26 May 2004 20:59:15 -0000 1.2
@@ -180,7 +180,7 @@
```

```
void cPipedMailMessage::SendString( const TSTRING& s )
{
- if( _fprintf( mpFile, s.c_str() ) < 0 )
+ if( _fprintf( mpFile, "%s", s.c_str() ) < 0 )
    {
        TOSTRINGSTREAM estr;
        estr << TSS_GetString( cTripwire,
tripwire::STR_ERR2_MAIL_MESSAGE_COMMAND )
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:pherman@frenchfries.net>
Paul Herman.

=====

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

=====

Securiteam: [UNIX] Tripwire Format String Vulnerability

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.