

[UNIX] Remote Format String Vulnerability in Tanne

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0027.html>

From: support@securiteam.com

Date: 01/08/03

From: support@securiteam.com

To: list@securiteam.com

Date: 8 Jan 2003 11:08:55 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Remote Format String Vulnerability in Tanne

SUMMARY

<<http://tanne.fluxnetz.de/>> Tanne is a small, secure session-management solution for HTTP. It replaces common sessions with a system consisting of PIN and TANs, well known from online banking. Its main purpose is to enable programmers of Web applications to have really secured sessions without cookies or session-ids. A vulnerability in the product allows remote attackers to cause the program to execute arbitrary code, by exploiting a format string vulnerability.

DETAILS

Vulnerable systems:

* Tanne version 0.6.17

Vulnerable code:

There is logger() function to 29 lines of 'netzio.c' code.

```
59 else
60 {
61 va_start( args, str );
```

Securiteam: [UNIX] Remote Format String Vulnerability in Tanne

```
62 vsnprintf( txt, 511, str, args );
63 va_end( args );
64 openlog( "Tanne2", LOG_PID, LOG_DAEMON );
65 syslog( LOG_INFO, txt ); // Here.
66 closelog();
67 }
68 umask( NORMALE_UMASK );
69 #else
70 va_start( args, str );
71 vsnprintf( txt, 511, str, args );
72 va_end( args );
73 openlog( "Tanne2", LOG_PID, LOG_DAEMON );
74 syslog( LOG_INFO, txt ); // Here.
75 closelog();
76 #endif
77 }
--
```

Patch:

```
--- netzio.c Wed Jul 25 22:17:29 2001
+++ netzio.patch.c Sun Jan 5 11:18:31 2003
@@ -62,7 +62,7 @@
vsnprintf( txt, 511, str, args );
va_end( args );
openlog( "Tanne2", LOG_PID, LOG_DAEMON );
- syslog( LOG_INFO, txt );
+ syslog( LOG_INFO, "%s", txt );
closelog();
}
umask( NORMALE_UMASK );
@@ -71,7 +71,7 @@
vsnprintf( txt, 511, str, args );
va_end( args );
openlog( "Tanne2", LOG_PID, LOG_DAEMON );
- syslog( LOG_INFO, txt );
+ syslog( LOG_INFO, "%s", txt );
closelog();
#endif
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:xploit@hackermail.com>>
dong-h0un yoU.

=====

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] Remote Format String Vulnerability in Tanne

=====
=====

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.