# IOActive Security Advisory

| | |
|---|---|
| **Title** | diskimages-helper band-size vulnerability |
| **Result** | Local Privilege Escalation (root) |
| **CVE ID** | CVE-2009-0150 |
| **Reported to Vendor** | September 30, 2008 |
| **Patch Released** | April 29, 2009 |
| **Author** | Tiller Beauchamp |

## Background

The diskimages-helper process enables the mounting of file systems. OS X's FileVault allows for the encryption of a user's home directories. Time Machine provides convenient, automatic backups of the file system. In order for FileVault and Time Machine to work efficiently together, the FileVault encrypted partition is split into smaller chunks; this allows encrypted partitions to be efficiently and routinely backed up in small pieces, rather than as one large file. These pieces are called bands.

## Attack Vector and Compromise

When a local, unprivileged user logs in with FileVault enabled, the diskimages-helper process launches and is responsible for mounting the user's home directory. This process runs as root and parses several user controlled files; in particular:

- `/Users/$user/$user.sparsebundle/Info.plist`
- `/Users/$user/$user.sparsebundle/bands/0`

While logged in, the user can edit these files in the `/Users/.$user/` directory, specifically crafting their values to cause a stack-based overflow that results in privileged code execution. During the user's next login, the diskimages-helper process attempts to read the crafted files and the payload is executed.

## Vulnerability

A signed-to-unsigned conversion flaw exists in diskimages-helper when it reads the band-size parameter. This value is stored in the user-specific XML configuration file `/Users/$user/$user.sparsebundle/Info.plist`. When the value specified for the band-size key is changed to a negative number, the diskimages-helper process crashes when the user attempts to log in:

```
Exception Type:  EXC_BAD_ACCESS (SIGSEGV)
Exception Codes: KERN_INVALID_ADDRESS at 0x00000000b0082000
Crashed Thread:  1

Thread 1 Crashed:
0   libSystem.B.dylib               0xffff061a __bzero + 26
1   com.apple.DiskImagesFramework   0x001997af
CBundleBackingStore::readDataFork(long long, unsigned long,
unsigned long*, void*) + 485
2   com.apple.DiskImagesFramework   0x001670ff
CEncryptedEncoding::copyHeaderInformation(CBackingStore*) + 369
```

For small, negative values of band-size, the application errors when it tries to zero-out past the stack boundary in a call to `bzero` (`memset`, actually):

```
memset(0xb0080358, 0, 4278617340)
```

As the negative number for band-size is decreased, the positive number that is passed to `bzero` also decreases. Eventually, the call to `bzero` does not write beyond the stack boundary and the `bzero` error does not occur. Next, the application copies the contents of `/Users/$user/$user.sparsebundle/bands/0` (hereafter referred to as `band0`) to a pointer value that points to a variable several stack frames back in the execution. This copy is performed with `pread` and the user controls the number of bytes to copy (multiple of 0x1000):

```
pread(fd:5, 0xb0080abc, size: 1794965504, offset: 0)
```

This overwrite completely corrupts multiple stack frames. For `band0` with random content, this results in memory access violations that involve the EAX register:

```
Exception Type:  EXC_BAD_ACCESS (SIGSEGV)
Exception Codes: KERN_INVALID_ADDRESS at 0x0000000063363134
Crashed Thread:  1

Thread 1 crashed with X86 Thread State (32-bit):
  eax: 0x63363134  ebx: 0x964adfa0  ecx: 0x964ae003  edx: 0x964adf92
  edi: 0x00000001  esi: 0x0000000e  ebp: 0xb00808c8  esp: 0xb00808c8
   ss: 0x0000001f  efl: 0x00010202  eip: 0x964ae010   cs: 0x00000017
   ds: 0x0000001f   es: 0x0000001f   fs: 0x0000001f   gs: 0x00000037
  cr2: 0x63363134
```

That register is controlled at offset 1420 within `band0`. Setting that value to something sane (such as 0) avoids the memory violation. The process proceeds with calculations, returning back through the stack trace until it hits our over-written `eip` value, which is found at offset 144 within `band0`:

```
Exception Type:  EXC_BAD_ACCESS (SIGSEGV)
Exception Codes: KERN_INVALID_ADDRESS at 0x00000000faceface
Crashed Thread:  Unknown

Unknown thread crashed with X86 Thread State (32-bit):
  eax: 0x00000000  ebx: 0x00165aad  ecx: 0x001a8481  edx: 0x00000000
  edi: 0x32303030  esi: 0x30300a62  ebp: 0x33203a30  esp: 0xb0080b50
   ss: 0x0000001f  efl: 0x00010246  eip: 0xfaceface   cs: 0x00000017
   ds: 0x0000001f   es: 0x0000001f   fs: 0x0000001f   gs: 0x00000037
  cr2: 0xfaceface
```

## Remediation

Apply Apple Security Update 2009-002 / Mac OS X v10.5.7 From Apple.

<http://support.apple.com/kb/HT3549>