

CVE-2019-3010 – Local privilege escalation on Solaris 11.x via xscreensaver

[Older >](#)

🕒 On 16 Oct, 2019 👤 By [Marco Ivaldi \(aka raptor\)](#)

As previously mentioned, [INFILTRATE](#) left me with the will to hack stuff and enjoy it like it was 1999. That's why I decided to take a closer look at **Solaris 11.4** and search for potential vulnerabilities. So one Sunday morning I started researching setuid root binaries in the default configuration and this happened...



raptor
@0xdea



It took just one Sunday morning of work to go from zero to 0day on a Solaris 11.4 box! I guess I haven't lost my swing 🦅🔧

to search type and hit enter

CATEGORIES

[Advisories](#)

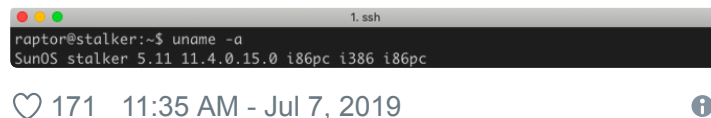
[Code](#)

[Notes](#)

RECENT POSTS

[CVE-2019-3010 – Local privilege escalation on Solaris 11.x via xscreensaver](#)

[Remote Desktop tunneling tips & tricks](#)



```
raptor@stalker:~$ uname -a
SunOS stalker 5.11 11.4.0.15.0 i86pc i386 i86pc
```

♥ 171 11:35 AM - Jul 7, 2019

💬 44 people are talking about this

Exploitation of a **design error vulnerability in xscreensaver**, as distributed with Solaris 11.x, allows local attackers to create (or append to) arbitrary files on the system, by abusing the -log command line switch introduced in version 5.06. This flaw can be leveraged to cause a **denial of service** condition or to **escalate privileges to root**, as shown in the following screenshot.

Graph's not dead

[CVE-2019-10149 exploit: local privilege escalation on Debian GNU/Linux via Exim](#)

[Raptor at INFILTRATE 2019](#)

POPULAR POSTS

[Universal Android SSL Pinning bypass with Frida](#)

[Brida: Advanced Mobile Application Penetration Testing with ...](#)

[Brida – A step-by-step user guide](#)

[Universal Android SSL Pinning Bypass #2](#)

[Reliable discovery and exploitation of Java deserialization ...](#)

ARCHIVES

[October 2019](#)

[June 2019](#)

[May 2019](#)

```

raptor@stalker:~$ uname -a
SunOS stalker 5.11 11.4.0.15.0 i86pc i386 i86pc
raptor@stalker:~$ id
uid=100(raptor) gid=10(staff)
raptor@stalker:~$ ./raptor_xscreensaver
raptor_xscreensaver - Solaris 11.4 LPE via xscreensaver
Copyright (c) 2019 Marco Ivaldi <raptor@0xdeadbeef.info>

X.Org X Server 1.19.5
Release Date: 2017-10-12
X Protocol Version 11, Revision 0
Build Operating System: SunOS 5.11 i86pc
Current Operating System: SunOS stalker 5.11 11.4.0.15.0 i86pc
Solaris ABI: 64-bit
Current version of pixman: 0.34.0
    Before reporting problems, check https://support.oracle.com/
    to make sure that you have the latest version.
Markers: (--) probed, (**) from config file, (==) default setting,
        (++) from command line, (!!) notice, (II) informational,
        (WW) warning, (EE) error, (NI) not implemented, (??) unknown.
(==) Log file: "/var/log/Xorg.1.log", Time: Tue Jul  9 14:58:36 2019
(==) Using system config directory "/usr/share/X11/xorg.conf.d"
(null): warning: could not set default locale
xscreensaver: 14:58:36: warning: $DISPLAY is not set: defaulting to ":0.0".
xscreensaver: 14:58:36: logging to file /usr/lib/secure/64/getuid.so
Oracle Corporation   SunOS 5.11   11.4   Aug 2018
You have new mail.
root@stalker:~# (II) Server terminated successfully (0). Closing log file.
id
uid=0(root) gid=0(root)
root@stalker:~# █

```

Example attack session

This vulnerability was confirmed on **Oracle Solaris 11.4 and 11.3 (X86 and SPARC)**. Previous Oracle Solaris 11 versions are also likely vulnerable.

Based on my analysis and on feedback kindly provided by [Alan Coopersmith](#) of Oracle, we concluded that this is a **Solaris-specific vulnerability**, caused by the fact that Oracle maintains a slightly different codebase from the upstream one. Alan explained this as follows:

[March 2019](#)
[November 2018](#)
[October 2018](#)
[July 2018](#)
[April 2018](#)
[February 2018](#)
[November 2017](#)
[October 2017](#)
[September 2017](#)
[July 2017](#)
[May 2017](#)
[February 2017](#)
[November 2016](#)
[October 2016](#)
[March 2016](#)
[February 2016](#)
[December 2015](#)
[May 2015](#)
[April 2015](#)
[March 2015](#)
[February 2015](#)
[February 2014](#)
[April 2011](#)
[February 2011](#)
[April 2010](#)

"The problem in question here appears to be inherited from the long-ago fork Sun & Ximian did to add a gtk-based unlock dialog with accessibility support to replace the non-accessible Xlib unlock dialog that upstream provides, which moves the uid reset to after where the log file opening was later added."

Specifically, the problem arises because of [this bit](#) of Solaris patches. As an interesting side note, it appears Red Hat [dropped this code](#) back in 2002.

Oracle has assigned the tracking# S1182608 and has **released a fix** for all affected and supported versions of Solaris in their Critical Patch Update (CPU) of [October 2019](#). Following Oracle's patch, an [advisory](#) and a Proof of Concept [exploit](#) have been published and are now available for download.

I would like to thank Alan Coopersmith and Ritwik Ghoshal of the [Oracle Security](#) team for their handling of my vulnerability report.

[January 2010](#)

[July 2009](#)

[February 2008](#)

[January 2008](#)

[October 2006](#)

[March 2006](#)

[April 2003](#)

META

[Log in](#)

[Entries](#) [RSS](#)

[Comments](#) [RSS](#)

[WordPress.org](#)

TAGS

[Advisory](#)

[Android](#)

[Brida](#)

[Burp Suite](#)

[Cachedump](#)

[Command Injection](#)

Related Posts



CVE-2019-2832
– Local privilege
escalation via
CDE dtprintinfo



CVE-2018-
14665 exploit:
local privilege
escalation on
Solaris 11



RunAsUser v0.5



Raptor at
INFILTRATE
2019



CVE-2016-7065
– Red Hat JBoss
EAP
deserialization
of untrusted
data



CVE-2016-5983
– IBM
WebSphere
deserialization
of untrusted
data

Written by: Marco Ivaldi (aka raptor) on October 16, 2019.

🔑 [Advisory](#) , [privilege escalation](#) , [Solaris](#) , [vulnerability](#) , [xscreensaver](#)

CVE-2003-0190

CVE-2009-2669

CVE-2010-3856

CVE-2018-14665

Exploit

facebook

frida

graph

HP System Management
Homepage

IBM AIX

IBM Websphere

iOS

Java

Java
deserialization

JBoss

Juniper

Id.so

LSASS.EXE

McAfee Virus
Scan Enterprise

Metasploit

mobile

MSSQL

ntlm

osint

password hashes

penetration
test

PowerShell

privilege
escalation

RunAsUser

Serialization

SIP digest leak

socmint

Solaris

SQL injection

SYN scan

vulnerability

warvox

Windows

X.org

