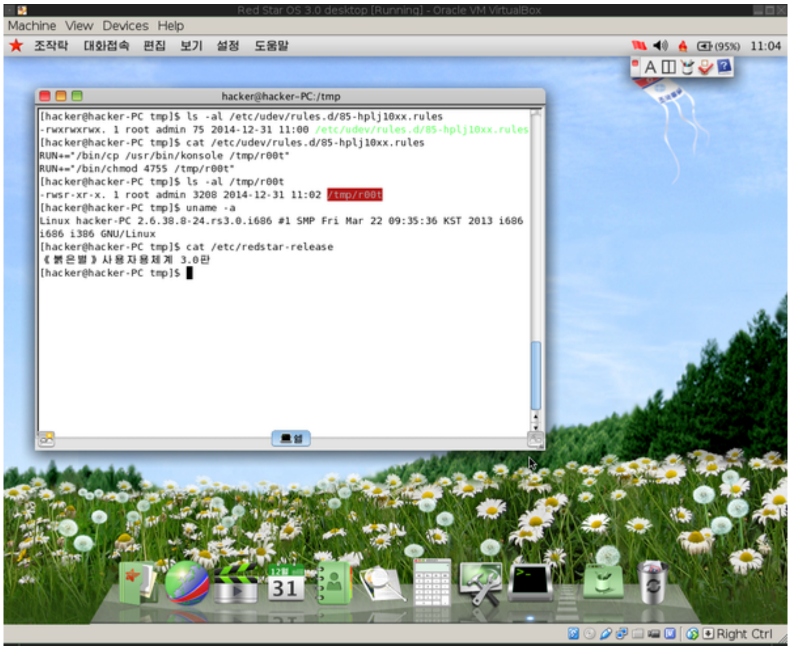
TECHNOLOGY LAB / INFORMATION TECHNOLOGY

Heads up, dear leader: Security hole found in North Korea's home-grown OS

Misconfigured default permissions on files create a way to get root on Red Star OS.

by **Sean Gallagher** - Jan 9, 2015 11:05am PST

62


Red Star OS 3.0 desktop [Running] - Oracle VM VirtualBox
Machine View Devices Help
조작탁 대화접속 편집 보기 설정 도움말
(95%) 11:04
hacker@hacker-PC:/tmp
31
Right Ctrl

```
[hacker@hacker-PC tmp]$ ls -al /etc/udev/rules.d/85-hplj10xx.rules
-rwxrwxrwx. 1 root admin 75 2014-12-31 11:00 /etc/udev/rules.d/85-hplj10xx.rules
[hacker@hacker-PC tmp]$ cat /etc/udev/rules.d/85-hplj10xx.rules
RUN+="/bin/cp /usr/bin/konsole /tmp/r00t"
RUN+="/bin/chmod 4755 /tmp/r00t"
[hacker@hacker-PC tmp]$ ls -al /tmp/r00t
-rwsr-xr-x. 1 root admin 3208 2014-12-31 11:02 /tmp/r00t
[hacker@hacker-PC tmp]$ uname -a
Linux hacker-PC 2.6.38.8-24.rs3.0.i686 #1 SMP Fri Mar 22 09:35:36 KST 2013 i686
i686 i386 GNU/Linux
[hacker@hacker-PC tmp]$ cat /etc/redstar-release
《붉은별》사용자용체계 3.0판
[hacker@hacker-PC tmp]$ 
```

Just a simple change to an unguarded file, and anyone who uses Red Star OS can get root. Of course, that's a pretty small population of potential hackers.

HackerFantastic

North Korea is a technological island in many ways. Almost all of the country's "Internet" is run as a private network, with all connections to the greater global Internet through a collection of proxies. And the majority of the people of the Democratic People's Republic of Korea who have access to that network rely on the country's official operating system: a Linux variant called Red Star OS.

Red Star OS, first introduced in 2003, was originally derived from Red Hat Linux. In theory, it gave North Korea an improved level of security against outside attack—a Security Enhanced Linux operating system based on Red Hat that could enforce strict government access controls on the few who got to use it.

However, because Red Star has had so few people with access to it, one of the ironic side effects has been that security holes in the operating system may have gone undetected. And as a security researcher who tested the latest release of Red Star's desktop version reported today, one flaw in the system would allow any user to elevate their privileges to those of the system's root account and bypass all those security policies put in place by the North Korean regime.

Red Star OS Desktop 3.0, which recently found its way onto torrents and various download sites as an .ISO image, is interesting for a number of reasons, including its attempt to look like Apple's Mac OS X

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Review: Mint 17.3 may be the best Linux desktop distro yet

If you don't want to think too hard about which OS you're using, Mint is for you.

WATCH ARS VIDEO

Ars visits Nest Labs

We learn about their programmable, self-learning, sensor-driven, Wi-Fi-enabled thermostats.

STAY IN THE KNOW WITH

LATEST NEWS

THAT ESCALATED QUICKLY

Martin Shkreli's other pharma company is dramatically collapsing

ROUNDTRIP TICKET TO THE IRON AGE

Scientists find 1500-year-old Viking settlement beneath new airport site

MINDLESS MUNCHING

Making healthy foods the default menu dupes people into eating better

Asian-American band "The

(earlier versions of Red Star mimicked Windows' user interface).

But as an anonymous researcher referring to himself as "Hacker Fantastic" noted in a post today to the Open Source Software Security (oss-sec) mailing list, it also has one significant security hole: a mistake made in permissions settings on a key file that allows anyone with access to the system to run commands as root. "Red Star 3.0 desktop ships with a world-writeable `udev` rules '/etc/udev/rules.d /85-hplj10xx.rules' which can be modified to include 'RUN+=' arguments executing commands as root by `udev.d`," the researcher wrote.

Udev.d is a generic kernel device manager that can identify hardware "hot-plugged" into a Linux system. The rules file determines how to handle the events associated with the connection of a new device and can include commands to be launched when certain devices are connected—commands that are run with system-level privileges. The "85-hplj10xx.rules" file is the ruleset associated with drivers for a USB-connected Hewlett Packard LaserJet 1000 series printer and is common to most Linux distributions.

That's probably not a device most North Koreans would typically hot-plug into their PCs. But because the permissions on that file are set as "world writable," any user regardless of permission levels could make changes to the rules to activate it for any device and execute any command they wanted with system-level privileges.

Ironically, there's a similar file permission error that the researcher discovered in Red Star OS 2.0's desktop version, in a different file that's even easier to abuse—the system configuration file for Linux's `rc` utility, which manages the operating system's boot-up. That vulnerability would allow anyone to add commands to be executed during system boot--a great way to ensure that surveillance software or other malware loads up persistently.

Configuration errors like these in the default installation of North Korea's official desktop operating system suggest that there are other security flaws to be found in Red Star. And the NSA may have already found them.

READER COMMENTS 62

Sean Gallagher / Sean is Ars Technica's IT Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.
@thepacketrat on Twitter

← OLDER STORY | NEWER STORY →

YOU MAY ALSO LIKE

Slants" overturns USPTO rule on "disparaging" trademarks

FOIA REINFORCEMENTS

Suspecting climate change conspiracy, Judicial Watch sues NOAA for scientists' e-mails

Progress! New CMOS chip can process both light and electricity