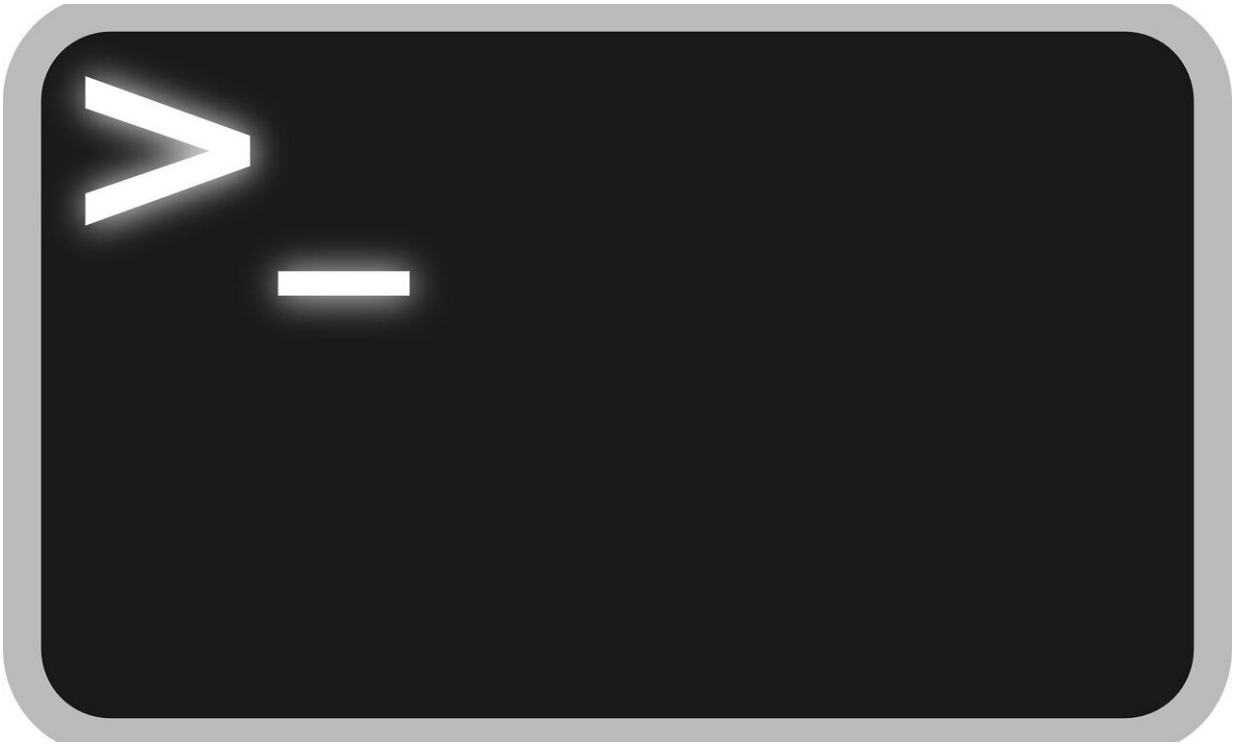
Patches to make Sudo utility less open to abuse

February 6 2020, by Nancy Cohen



Credit: CC0 Public Domain

A flaw that gave out root privileges gets patched. It is a utility that, said Dan Goodin in *Ars Technica,* can be found in "dozens of Unix-like operating systems."

The patch is for a "potentially serious bug," said Goodin, where

unprivileged users can take on root privileges on vulnerable systems.

This is all about Sudo, a "very popular, very simple" sysadmin application, said *ZDNet*.

Sudo is used in a range of Linux and Unix-based systems, including Apple macOS. Apple released a patch update for macOS High Sierra 10.13.6, macOS Mojave 10.14.6, macOS Catalina 10.15.2, wrote Mohit Kumar in *The Hacker News*.

Sudo, said Stephen Vaughan Nichols in ZDNet, is easy to abuse. Yet another way of saying it, in *ZDNet*: "it's so darn useful, until it's not."

Sudo has weight as "one of the most important, powerful, and commonly used utilities that comes as a core command pre-installed on macOS and almost every UNIX or Linux-based operating system," said Kumar. Malcolm Owen in *AppleInsider* also talked about Sudo in general. It has the potential to cause havoc if misused.

"The vulnerability, tracked as CVE-2019-18634, is the result of a stack-based buffer-overflow bug found in versions 1.7.1 through 1.8.25p1," said *Ars Technica*. "It can be triggered only when either an administrator or a downstream OS, such as Linux Mint and Elementary OS, has enabled an option known as pwfeedback."

In the vulnerable versions, an attacker could take advantage of a pair of separate flaws in order to gain root privileges. The problem was not just a "Mac thing" but *AppleInsider* made note that the vulnerability was found by an Apple security employee Joe Vennix.

Decipher: "The risk of exploitation is quite high for systems on which the pwfeedback option is enabled. In order to exploit the bug, an attacker would just need to send a large amount of data to sudo through

the password prompt field. The vulnerability results from two separate errors in the sudo code."

"Most distros, though, are unaffected," said *The* Register, "unless defaults were changed, but do check." The security hole is only active if the pwfeedback option is enabled and a few Linux distributions—seemingly Mint and Elementary OS—do enable the option, said Tim Anderson; he added that pwfeedback was generally disabled by default.

Steven Vaughan-Nichols in *ZDNet* expanded on that: In CVE-2019-18634, Apple Information Security researcher Joe Vennix discovered that if the "pwfeedback" option was enabled in a sudoers configuration file, "any user, even one who can't run sudo or is listed in the sudoers file, can crack a system."

The bug problem has a relevant history. "The sudo version history shows that the vulnerability was introduced in 2009 and remained active until 2018, with the release of 1.8.26b1," said *Ars Technica*.

Softpedia's Bogdan Papa also explained what was going on. The "sudo" vulnerability flaw involved the "pwfeedback option, enabled by default on distros like Linux Mint and elementary OS. Because of the bug, any user can trigger a stack-based buffer overflow even if they aren't listed in the sudoers file."

Enter the release of version 1.8.31. The maintainers of Sudo released sudo version 1.8.31 with a patch. This includes a patch to block the exploit, said Papa, "but if installing this latest release isn't possible, disabling pwfeedback is the easiest way to stay secure. Only devices where pwfeedback is enabled are exposed to attacks."

Owen expanded on what *AppleInsider* readers should do about keeping

their machines secure. Those who want to know if their Mac is still affected can check out his article in AppleInsider.

Fossbytes had this helpful tip on Tuesday: "In case, you're running the exploitable version of Sudo, patches are now available for Ubuntu Linux systems, Linux Mint, and elementary OS."