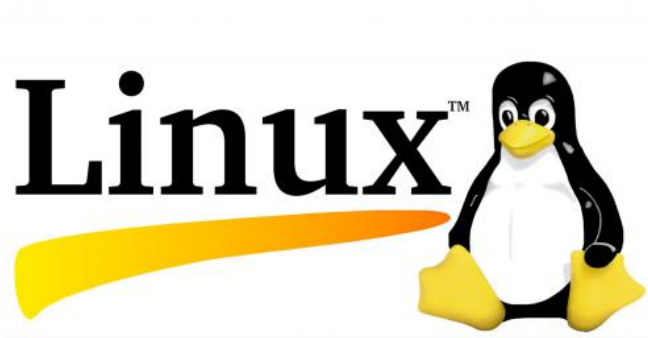
Linux kernel vulnerability traced to keyring implementation

21 January 2016, by Nancy Owano



Security watchers this week focused on the zero-day vulnerability which was found inside the Linux kernel. *Geektime*'s Gabriel Avner and Yaneev Avital reported Tuesday that the Israeli cyber security firm Perception Point found the Linux code vulnerability. The news was not trivial. And it was not good.

It puts 66 percent of Android devices and "tens of millions" of machines at risk for intruders to get control.

The exploit resides in the core kernel, said *Geektime*. (The core kernel, fundamental to an operating system, manages input/output requests from software and translates them into data processing instructions. To quote the *Android Developer Guide*: "A kernel is a critical component of every Operating System. It can be seen as a sort of bridge between the applications and the actual hardware of a device. Usually the data processing part is done at hardware level, furthermore the kernel is the most low-level abstraction layer for the resources.")

Avner and Avital said they learned it was found in the "keyring feature that runs on systems operating Linux's 3.8 software and above." The bug is described as coming from a reference leak in the keyrings facility.

Here is the statement from Perception Point:

"The Perception Point Research team has identified a 0-day local privilege escalation vulnerability in the Linux kernel. While the vulnerability has existed since 2012, our team discovered the vulnerability only recently, disclosed the details to the Kernel security team, and later developed a proof-of-concept exploit. As of the date of disclosure, this vulnerability has implications for approximately tens of millions of Linux PCs and servers, and 66 percent of all Android devices (phones/tablets). While neither us nor the Kernel security team have observed any exploit targeting this vulnerability in the wild, we recommend that security teams examine potentially affected devices and implement patches as soon as possible."

What does Android have to do with all this? Because Android uses the Linux kernel, the vulnerability is also present in all Android devices running KitKat or higher, which accounts for about 66 percent of current users, said Fahmida Rashid, who covers information security for *InfoWorld*.

Vlad Dudau, news editor, *Neowin*, found it ironic that "the flaw itself was found to be part of one of Linux's security features and it relates to the way processes store secure information in keyrings."

The security team thanked "David Howells, Wade Mealing and the whole Red Hat Security team for that fast response and the cooperation fixing the bug." Most Linux distributions have already made the patch available, said Steven Vaughan-Nichols in *ZDNet*.

Perception Point's CEO Yevgeny Pats, in *Geektime*, said that Red Hat's patch should be enough to insulate vulnerable devices, but many

older machines no longer update automatically, leaving them open to the exploit if left unattended. *Geektime* said he recommended that all Android and Linux users update their devices as soon as possible. The researchers contacted other Linux distributors about the vulnerability too.

What does the flaw actually enable the intruder to do? Dudau of *Neowin* said the flaw allows an attacker to gain root level privileges by running a piece of malware on an affected device. With that elevation of privileges the attacker could take complete control of a device and its data.

Damage so far? No evidence of any, according to reports. The exploit has not been found in the wild as of now. Perception Point's Pats said in *Geektime* that he was unaware of any malware using this vulnerability to carry out attacks.

Neowin commented on damage risks. There is less to worry about on the PC side of things, said *Neowin*, "where Red Hat, SUSE, and the Linux security teams are already in the middle of deploying patches to fix this vulnerability."

Henry Casey in *Tom's Guide* delivered advice for Android users about this: don't download apps from sources other than the Google Play Store; run system updates when your carrier or phone maker pushes them down to your device. If planning to buy an Android phone, make sure its manufacturer issues regular or monthly security updates.

The team identified the vulnerability while they were developing their security agent for Linux systems, said *Geektime*.

More information: perception-point.io/2016/01/14 … ility-cve-2016-0728/

APA citation: Linux kernel vulnerability traced to keyring implementation (2016, January 21) retrieved 23 April 2021 from https://techxplore.com/news/2016-01-linux-kernel-vulnerability-keyring.html