Zero-day privilege escalation disclosed for Android

reader comments

46 with 30 posters participating

Share this story

Researchers have disclosed a zero-day vulnerability in the Android operating system that gives a major boost to attackers who already have a toe-hold on an affected device.

The privilege-escalation flaw is located in the V4L2 driver, which Android and other Linux-based OSes use to capture real-time video. The vulnerability results from a “lack of validating the existence of an object prior to performing operations on the object,” researchers with Trend Micro’s Zero Day Initiative said in a blog post published Wednesday. Attackers who already have untrusted code running with low privileges on a device can exploit the bug to access privileged parts of the Android kernel. The severity score is rated a 7.8 out of a possible 10 points.

Modern OSes have become increasingly hard to compromise in recent years thanks to exploitation mitigations that prevent untrusted code from interacting with hard drives, kernels, and other sensitive resources. Hackers have responded by chaining two or more exploits together. A buffer overflow, for instance, may allow an attacker to load malicious code into memory, and a privilege-escalation flaw gives the code the privileges it needs to install a persistent payload.

The net result of all of this: privilege-escalation bugs are increasingly valuable, as demonstrated by the so-called Dirty Cow vulnerability discovered affecting Linux in 2016. Within days of being discovered, the privilege-escalation bug was being used to root Android devices. A year after coming to light, Dirty Cow was being exploited by malicious apps to bypass security protections built into Android.

“This vulnerability is similar to Dirty Cow in that it is in the core code of the kernel, so it would apply to all Android devices,” Christoph Hebeisen, director of security intelligence at mobile security provider Lookout, told Ars. “However, an exploit based on this vulnerability would not be as elegant as DirtyCow and probably not quite as reliable.”

Based on the advisory, Hebeisen said it appears only apps or code that already have access to the V4L subsystem used by an attached camera could exploit the flaw. Dirty Cow, by contrast, resided in a core memory-management feature. What’s more, exploiting the flaw was relatively easy, a trait that made exploits highly reliable.

ZDI’s Wednesday post said researchers notified Google of the vulnerability in mid-March and that by the end of June, the company had confirmed that the flaw would be fixed. When ZDI asked Google for an update last month, Google responded there would be no further updates. Google released the Android Security Bulletin for September on Tuesday, and the flaw still wasn’t fixed. Google didn’t respond to a request for comment.

“Given the nature of the vulnerability, the only salient mitigation strategy is to restrict interaction with the service,” ZDI researchers wrote in Tuesday’s post. “Only the clients and servers that have a legitimate procedural relationship with the service should be permitted to communicate with it.”

In an email, ZDI Director Brian Gorenc said Android users

should limit the apps they install and ensure the apps come only from Google Play. He said ZDI verified the flaw affected the latest versions of Android.

https://arstechnica.com/?p=1562969