engadget

Security

Google discloses 'high severity' Mac security flaw ahead of patch

The vulnerability could let attackers mess with the file system in secret.

Jon Fingas, 03.04.19

Google's Project Zero security disclosure program is once again proving to be a double-edged sword. The company has detailed a "high severity" macOS kernel flaw that lets people modify a user-mounted file system image without the virtual management subsystem being any the wiser, theoretically letting an attacker go unnoticed by users. Apple is working on a patch, but the disclosure ahead of the fix could leave Mac users vulnerable until it's ready.

The less-than-ideal timing stems in part from how Project Zero works. Google notified Apple of the bug in November 2018, but its automatic 90-day disclosure policy means that it will publicize security vulnerabilities whether or not a fix is in place. While the company does offer a 14-day grace period for companies who don't think they'll have patches ready in time, Apple didn't necessarily qualify for this reprieve. We've asked both Apple and Google for comment.

It's not clear how easy this would be to exploit in the wild. In the meantime, you'll likely want to be particularly careful about the sites you visit and the files you download. A successful attack could theoretically make serious changes to macOS without tripping system-level safeguards, and you might not be aware of the damage until considerably later.

Acer ConceptD 9 laptop hands-on: A bombastic attempt to stand out

Cherlynn Low

23m ago

Fox Sports lands US broadcast rights to 'FIFA 19' eSports events

Kris Holt
35m ago

An Instagram bug briefly showed Stories to strangers

Christine Fisher

43m ago

Nepal bans 'PUBG' over concerns kids are addicted

Kris Holt

55m ago

'Wine Country' is an 'SNL' reunion disguised as a movie

AJ Dellinger

1h ago