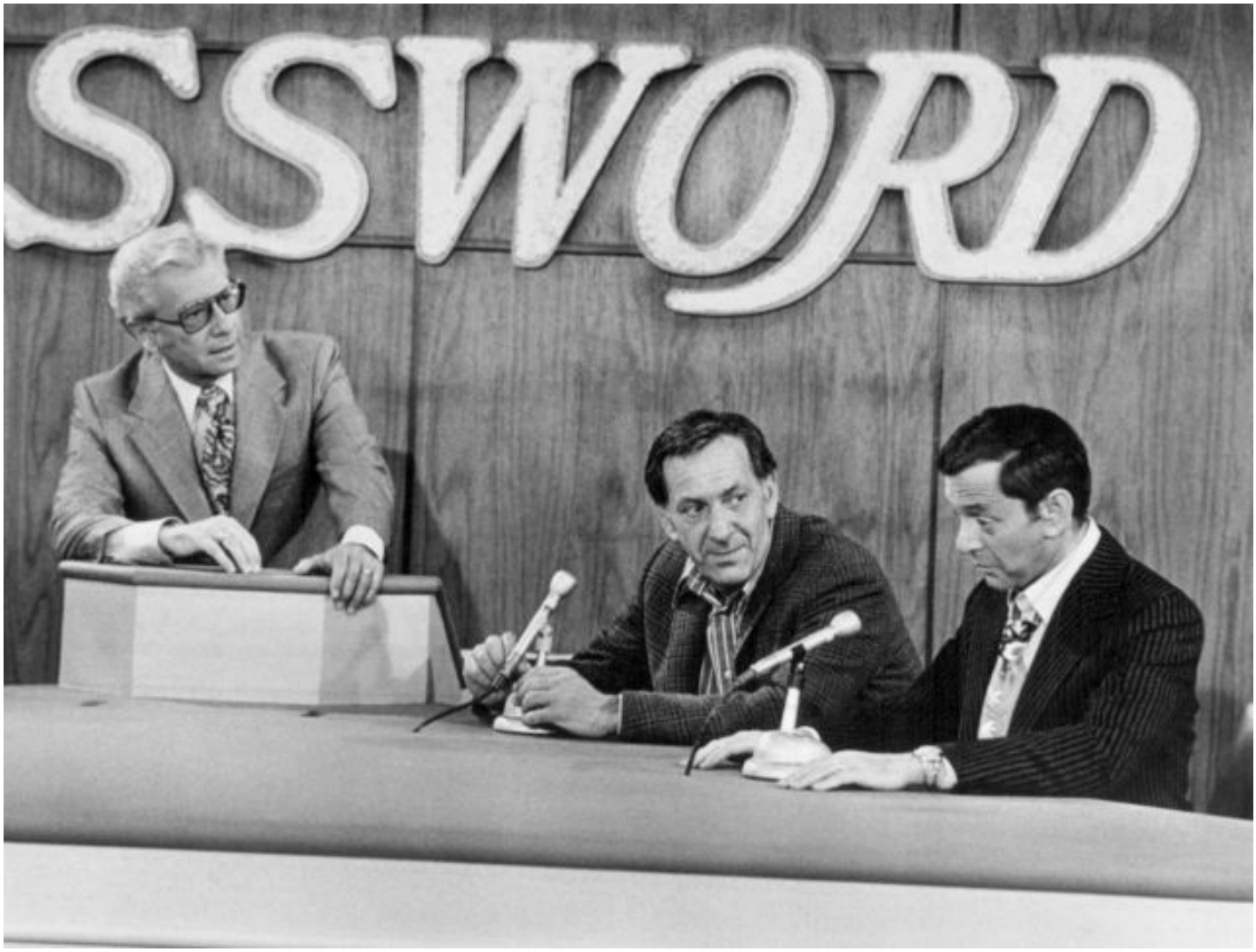
RISK ASSESSMENT —

Potent LastPass exploit underscores the dark side of password managers

Developers are scrambling to fix flaw that allows theft, malicious code execution.

DAN GOODIN - 3/28/2017, 12:06 PM



Wikimedia

Developers of the widely used LastPass password manager are scrambling to fix a serious vulnerability that makes it possible for malicious websites to steal user passcodes and in some cases execute malicious code on computers running the program.

The flaw, which affects the latest version of the LastPass browser extension, was briefly described on Saturday by Tavis Ormandy, a researcher with Google's Project Zero vulnerability reporting team. When people have the LastPass binary running, the vulnerability allows malicious websites to execute code of their choice. Even when the binary isn't present, the flaw can be exploited in a way that lets malicious sites steal passwords from the protected LastPass vault. Ormandy said he developed a proof-of-concept exploit and sent it to LastPass officials. Developers now have three months to patch the hole before Project Zero discloses technical details.

"It will take a long time to fix this properly," Ormandy said. "It's a major architectural problem. They have 90 days, no need to scramble!"

In a blog post published Monday, LastPass officials thanked Ormandy for alerting them to the bug and said a fix was on the way. In the meantime, they said LastPass users should protect themselves by entering stored passwords into websites using the LastPass vault as a launch pad for opening

"This attack is unique and highly sophisticated," the blog post warned. "We don't want to disclose anything specific about the vulnerability or our fix that could reveal anything to less sophisticated but nefarious parties. So you can expect a more detailed post mortem once this work is complete."

The vulnerability is the third one Ormandy has privately reported to LastPass this month. Last week, he described bare-bones details of two different flaws found in LastPass extensions for multiple browsers. LastPass developers quickly implemented changes on their server that made the flaws harder to exploit and released patches two days later.

The string of vulnerabilities underscores the tradeoff that comes from use of any password manager. Storing dozens, hundreds, or even thousands of passwords in a single place poses catastrophic risks should that resource be breached. Exploits become easier by convenience features that, for example, store encrypted password vaults in Internet-accessible locations or automatically paste passwords into websites. Ultimately, password managers likely make the average user safer because they make it possible to use long, complex, and unique passwords. And that protects people in the event that their password is exposed in website breaches, which are much more common than real-world password manager exploits.

DAN GOODIN
Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 247

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

Russia's hack of State Department was "hand-to-hand" combat

Charter won't have to compete against other ISPs thanks to FCC decision

iOS 10.3.1 includes bug fixes and improves the security of your iPhone or iPad

DOJ warns companies seeking H-1B visas: Don't discriminate against US citizens

Tesla delivers 25,418 vehicles in 2017's first quarter as EV market grows

HTC Vive's first-ever price drop lasts just one day this week

Brain cancer patients live longer wearing electric cap designed to zap tumors

After vote to kill privacy rules, users try to "pollute" their Web history