RISK ASSESSMENT —

Firefox and Tor release urgent update for 0-day that's under active attack

Critical code-execution flaw resides in Windows, Mac, and Linux. Patch now.

DAN GOODIN - 11/30/2016, 1:20 PM

Developers with both Mozilla and Tor have published browser updates that patch a critical Firefox vulnerability being actively exploited to deanonymize people using the privacy service.

FURTHER READING
Firefox 0-day in the wild is being used to attack Tor users

"The security flaw responsible for this urgent release is already actively exploited on Windows systems," a Tor official wrote in an advisory published Wednesday afternoon. "Even though there is currently, to the best of our knowledge, no similar exploit for OS X or Linux users available, the underlying bug affects those platforms as well. Thus we strongly recommend that all users apply the update to their Tor Browser immediately."

The Tor browser is based on the open-source Firefox browser developed by the Mozilla Foundation. Shortly after this post went live, Mozilla security official Daniel Veditz published a blog post that said the vulnerability has also been fixed in a just-released version of Firefox for mainstream users. On early Wednesday, Veditz said, his team received a copy of the attack code that exploited a previously unknown vulnerability in Firefox.

FURTHER READING
Attackers wield Firefox exploit to uncloak anonymous Tor users

The attack executed code when targets loaded malicious JavaScript and code based on scalable animation vector graphics. The exploit used the capability to send the target's IP and MAC address to an attacker-controlled server. The code in general resembles the types of so-called network investigative techniques used by law-enforcement agencies, and specifically one that the FBI used in 2013 to identify Tor-protected users who were trading child pornography.

A "threat to the broader Web"

"This similarity has led to speculation that this exploit was created by FBI or another law enforcement agency," Veditz wrote. "As of now, we do not know whether this is the case. If this exploit was in fact developed and deployed by a government agency, the fact that it has been published and can now be used by anyone to attack Firefox users is a clear demonstration of how supposedly limited

government hacking can become a threat to the broader Web."

According to the release notes for version 50.0.2 released in the past few hours, the underlying vulnerability is indexed as CVE-2016-9079 and is rated as critical. A separate Mozilla security advisory shows that it also affects Mozilla's Thunderbird e-mail application, as well as the Firefox Extended Support release version used by the Tor browser.

Attack code exploiting the vulnerability first circulated Tuesday on a Tor discussion list and was quickly confirmed as a zero-day, the term given to vulnerabilities that are actively exploited in the wild before the developer has a patch in place. The malicious payload delivered by the code-execution exploit is almost identical to one the FBI used in 2013 to identify people who were trading child pornography on a Tor-anonymized website. Because the initial post to the Tor group included the complete source code, the highly reliable exploit quickly became available to millions of people, although they would have to make minor changes to make use of it.

Besides an update for Firefox, Wednesday's Tor release also includes an update to NoScript, a Firefox extension that ships with the Tor browser. NoScript allows users to select the sites that can and cannot execute JavaScript in the browser. For privacy and usability reasons, the Tor browser has traditionally installed NoScript in a way that allowed all sites to run JavaScript in the browser. It's not clear what effect the new NoScript update has on that policy.

Firefox and Tor users should install the fixes at once. People using both Tor and mainstream versions of Firefox are believed to be protected from the attack by setting the Firefox security slider to "High," although the setting will prevent many sites from working as expected. For much more about this attack see Ars's previous coverage Firefox 0-day in the wild is being used to attack Tor users.

Post extensively updated throughout to add details about a just-released patch for the mainstream version of Firefox and Mozilla comments about the exploit.

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 21 SHARE THIS STORY

← PREVIOUS STORY NEXT STORY →

Related Stories

Today on Ars