

Google had Zero-Day reasons for shouting about updates

March 8 2019, by Nancy Cohen



Credit: CC0 Public Domain

Update. Now. This minute. Don't go until you do it. That was the pushy message from Google on Thursday. A Zero-Day exploit was at play against the Chrome browser and there was no wiggle room for users to ignore it until they were in a better mood.

By Thursday, *Fossbytes*, *ZDNet* and other tech watching sites were all over the story. Chrome is a hugely popular [browser](#) and Google is quite successful in its branding as a relatively safe keeper of Chrome. So any story to the contrary made instant news.

You were safe if your update check to see if you had the latest was showing up as Version 72.0.3626.121.

Who had discovered the CVE-2019-5786 [security](#) flaw? Clement Lecigne of Google's Threat Analysis Group was named.

Lecigne wrote on the Google Security Blog. "To remediate the Chrome vulnerability (CVE-2019-5786), Google released an update for all Chrome platforms on March 1; this update was pushed through Chrome auto-update. We encourage users to verify that Chrome auto-update has already updated Chrome to 72.0.3626.121 or later."

So, they were talking about the kind of exploit "in the wild," unknown, without a patch, capable of unleashing complications.

As Kaspersky Lab explains the meaning of zero-day, "Usually the program creators are quick to create a fix that improves program protection, however, sometimes hackers hear about the flaw first and are quick to exploit it. When this happens, there is little [protection](#) against an

attack because the software flaw is so new."

Or, as *Naked Security* puts it, this is "a vulnerability that the Bad Guys figured out how to exploit before the Good Guys were able to find and patch it themselves—where "even the best- informed sysadmins had zero days during which they could have patched [proactively](#)."

This was no fun experiment; Google was aware of the vulnerability being exploited in the wild. Andrew Whalley tweeted, Take a moment to check you are running the latest Chrome.

Justin Schuh, Google Chrome security lead, was also sounding the trumpet for Chrome users to check for the update. His tweet by March 5 was a we're-not-playing public announcement: "...seriously, update your Chrome installs...like right this minute." Why, what's the rush? Because Chrome Zero-Day was under active attacks. Catalin Cimpanu in *ZDNet* said the patched bug was under [active](#) attacks at the time of the patch.

Adash Verma in *Fossbytes* said, "While the details are scarce, we know that the flaw deals with memory management in Chrome's Filereader, which is an API that lets [web apps](#) read the content of files stored on user's [computers](#)."

Schuh tweeted: "This newest exploit is different, in that initial chain targeted Chrome code directly, and thus required the user to have restarted the browser after the update was downloaded."

At what level was the CVE-2019-5786 threat? it has been labeled as "High." *ZDNet* said Google described the security flaw as a memory management error in Google Chrome's FileReader—a web API that lets web apps read the contents of files stored on the user's computer.

Here is what Abner Li explained in *9to5Google*. "This particular attack

involves the FileReader API that allows websites to read local files, while the 'Use-after-free' class of vulnerabilities—at worse—allows for execution of malicious [code](#)."

What does that mean, use-after-free vulnerability? A type of memory error comes along when an app tries to access memory after it has been freed/deleted from Chrome's allocated memory, said Cimpanu. He added that the flow involved a memory management error in Google Chrome's FileReader. Cimpanu said the web API was included in major browsers whereby web apps read the contents of files stored on the user's computer.

He said an incorrect handling of this type of memory access operation can lead to the execution of malicious code.

Long and short, Google came out with a fix for the zero day flaw. Long and short, a fix has already been issued

Google stated that "Access to bug details and links may be kept restricted until a [majority](#) of users are updated with a fix. We will also retain restrictions if the bug exists in a third party library that other projects similarly depend on, but haven't yet fixed."

In the bigger browser security picture, tech watchers are likely to still regard Chrome as one of the safest around. *DataHand* made a point that "The search engine [giant](#) has invested a lot of resources in securing the browser in recent years and there haven't been many security breaches."

Nonetheless, the security environment has to survive on a cardinal rule: Never say never to the possibility of new attacks. Which browser is entirely foolproof? Worth watching, though, is how skillful the browser owners can be in addressing threats and issuing solutions.

Ryan Whitwam, *ExtremeTech*: "Browsers contain so much of our digital lives now that any vulnerability is potentially disastrous. Luckily, it's very rare that nefarious online individuals will spot a serious vulnerability before Google or outside security *researchers*...It was Google's own Threat Analysis Group that spotted the flaw in Chrome on Feb. 27."

© 2019 Science X Network

Citation: Google had Zero-Day reasons for shouting about updates (2019, March 8) retrieved 9 April 2024 from <https://techxplore.com/news/2019-03-google-zero-day-shouting.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.