Chrome targeted by Magnitude exploit kit

blog.malwarebytes.com/exploits-and-vulnerabilities/2021/10/magnitude-ek-has-been-spotted-targeting-the-chrome-browser/

Pieter Arntz October 21, 2021

Exploit kits (EK) are not as widespread as they used to be. One of the reasons is likely that most exploit kits targeted software that is hardly ever used anymore. Internet Explorer, Silverlight, and Flash Player to name a few, have been deprecated, replaced, and quickly lost their user-base.

So, just when you start thinking there is one less threat to worry much about, researchers have found an exploit kit with a keen interest in Chrome. Which, from a business point of view, makes a lot of sense, since Chrome is close to becoming not just a market leader, but almost a monopolist in the browser market.

Chrome has, at the time of writing, a market share of around 65%. The only other browser that reaches a market share that is over 10% is Safari. So if you are in the business of compromising browsers that visit your website or watch your advertisement, having Chrome users on your target list is a big plus.

Or, as Malwarebytes' Director of Threat Intelligence, Jérôme Segura, put it:

> "The future of exploit kits is via Chrome exploits. This could either be an anomaly or the beginning of a new era with big implications for the years to come."

Magnitude EK

Enter the Magnitude exploit kit. Researchers have found that the Magnitude EK is actively using two vulnerabilities to exploit Chromium-based browsers. Magnitude is used in malvertising attacks to infect victims who visit compromised websites and its payload of choice is the Magniber ransomware.

The vulnerabilities

CVE-2021-21224 is described as a type confusion in V8 in Google Chrome prior to 90.0.4430.85 which allows a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. V8 is Google's open source high-performance JavaScript and WebAssembly engine. This vulnerability was patched in April.

CVE-2021-31956 is a Windows NTFS Elevation of Privilege (EoP) vulnerability. This vulnerability can be used in combination with CVE-2021-21224 to escape the Chromium sandbox. This vulnerability was patched in June.

PuzzleMaker

Practically the same combination of vulnerabilities was described in June when Microsoft fixed seven zero-days, including the CVE-2021-131956 we mentioned earlier. Back then, the attacker using these vulnerabilities was dubbed PuzzleMaker. At the time it was unknown which Chrome vulnerability was used by the attacker, but it's highly likely that it was the same as Magnitude has been found leveraging now.

Payload

There is no malicious payload attached to the Magnitude exploits yet, the attack just exfiltrates the victim's Windows build number. But reportedly, this is Magnitude EK's standard procedure to test out new exploits, so this could change quickly if they start to see positive results.

How to protect yourself

It is only on rare occasions that we write about vulnerabilities and then tell you there isn't much to worry about. But in this case, the only people that have anything to worry about are Windows users that browse the web using Chrome or Chromium based browsers (like Edge), but have disabled its automatic updates and haven't updated since April. You would also have to run on a non-updated Windows system since June, or run Chrome with the *–no-sandbox* switch (not recommended). And even then all that would happen if you ran across the Magnitude EK (which usually focuses on South Korea) is getting fingerprinted.

But you do understand that you should update your OS and browser nonetheless, right?

Enable automatic updates

If you want to save yourself the trouble of manually installing updates, there are a few things you can do. For Google Chrome (under Windows) you can choose this page as one of the tabs that opens when you run the browser: *chrome://settings/help*. If there has been an update since the last time you closed your browser, this page will alert you and initiate a download of the update.

In Windows 10 you can select the Start button, then select *Settings* > *Update & security* > *Windows Update*. Select *Advanced options*, and then under *Choose how updates are installed*, select *Automatic (recommended)*.

Stay safe, everyone!