COMPUTER NEWS from the

As found on the web and other sources!

Chrome Zero-Day Bug: Update Now

By John Lister on March, 4 2021 in “Infopackets.com”.

If you use Chrome, you need to make sure it's up to date. The browser has been hit by a dreaded zero-day flaw.

In this case, hackers are aware of the bug and are actively exploiting it before Google has a chance to issue a security patch. The name comes from the fact that Google has "zero days" head start in getting the patches out.

Google confirmed that it "is aware of reports that an exploit for CVE-2021-21166 [the bug in question] exists in the wild." (Source: googleblog.com)

High Severity Flaw

The security flaw is rated as "high severity" on Google's rankings of how much damage it could do. That's the second highest level, below only "critical".

Examples of damage at this level include attackers running code on a computer or reading data without permission. In this case, a computer connected to the Internet running the Chrome browser is all that is needed to be infected with malware.

It can also cover cases where an attacker can read or alter key system data (such as the file system or registry) but where a mitigating factor limits the potential damage.

As often happens, Google has kept exactly what the vulnerability entails under wraps, a policy it believes will reduce the risk of tipping off even more hackers about what the bug is or how to exploit it. It's simply described it as "Object lifecycle issue in audio" and following a link for more details brings up an error message. (Source: tomsguide.com)

Close Chrome To Update

The good news is that Chrome will normally automatically apply the security fix whenever it is closed and closed and reopened. Users may need to close all Chrome tabs and windows to trigger this.

Given the severity and zero-day nature of this bug, it may be worth double-checking the browser is up to date. To do this, users can click on the settings menu icon, which is the three vertical dots in the top right corner of Chrome, just below the X button for closing the browser.

From here, users should click "Settings" and then "About Chrome" on the following screen. The screen then either show a blue tick and a note that "Google Chrome is up to date" or show an option to update the browser.

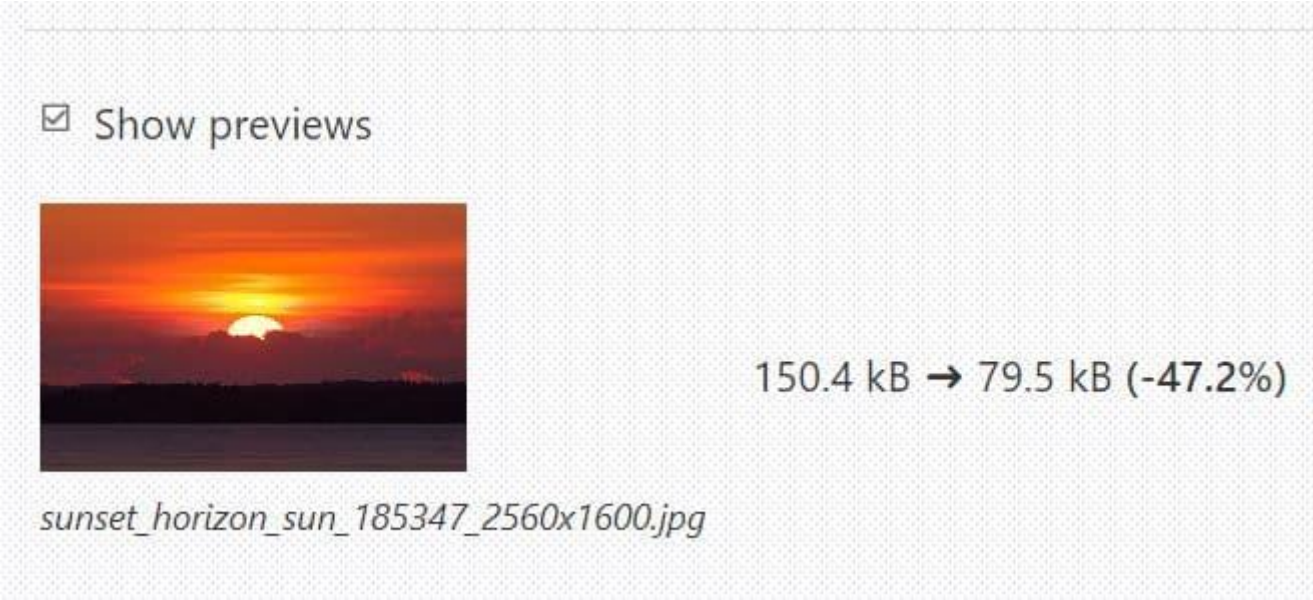
What's Your Opinion?

Do you use Chrome? Do you pay any attention to updates or leave it to take care of itself? What's the longest you usually leave browser windows open for?

From Gizmo’s Freeware.

This JPG Optimizer Works Entirely in Your Browser

Last updated by rhiannon on 05. February 2021 - 08:03



This privacy focused image optimizer work in your browser, images never leave your device. All image processing is done entirely in your browser.

JPEG.rocks is a new online app that optimizes image in your browser online or offline. It doesn't use persistence storage: no cookies and no local browser storage. JPG is the only format supported right now.

The interface is clean and easy to use. Upload or drag and drop files, and download the optimized images. To change the image quality (default is 75), click on Settings and use the slider bar.

If you want a privacy focused easy way to optimize JPG files online and off, this is a good choice. Currently, results are lossy (that will likely change in the future) but is entirely acceptable for most web and home uses.
If you need something with higher quality output and more options check out our article on Squoosh by Google – it works entirely in your browser too.

Apple Suffers Malware Scare

By John Lister on March, 2 2021 in “Infopackets.com”.

Apple says it has dealt with the risk from a newly-discovered piece of malware affecting macOS. It's a reminder that macOS isn't completely immune from malware - which may have been the point of the attack.

Security company Red Canary discovered the malware and dubbed it Silver Sparrow. It says data from Malware bytes showed it was present on 29,139 computers. (Source: redcanary.com)

It appeared to target computers which have the M1 chip. That's an Apple produced processor designed specifically for Macs. It's combines multiple functions on a single chip, the idea being to increase efficiency and make the computer carry out key operations much more quickly.

Apple was able to stop the spread of Silver Sparrow because it uses digitally signed security certificates for software developers (similar to how HTTPS works) to authenticate and prove software has not been modified and is therefore not malicious. It was able to revoke the digital certificates for the account used to deliver the malware, meaning in theory the installation would fail and not install on any new machines.

Malware 'Phones Home' Hourly

Most common malware on Macs is designed to deliver unwanted ads, often to scam money from advertisers who don't realize their ads are being shown in an underhanded way that's unlikely to bring great results.

However, researchers say Silver Sparrow had the potential to be more serious. It's designed to hide itself and even self-destruct if necessary. It also checks a "command-and-control" server hourly to see if the creators have issued any new instructions. That could allow it to deliver more dangerous malware to the already-infected machine.

One possibility is that the creators simply weren't quick enough to exploit this potential before Silver Sparrow was discovered. Another theory is that the creators were simply demonstrating their ability to breach Mac security. (Source: bbc.co.uk)

Age Old Debate

How secure Macs are compared to Windows PCs is an oft-debated topic in the tech world. One argument is that the way the operating system and software works is inherently more secure (and less buggy) than Windows.

The counter-argument is that attackers simply put more of their energy into Windows PC because the potential pool of machines to infect and exploit is much greater. In reality, it's probably a combination of the two.

What's Your Opinion?

Do you use a Mac? Do you feel Macs are fundamentally more secure than Windows PCs? Does that lead Mac users to be more relaxed about following good security practices?

NO COMMENT

Half of us are going to come out of this quarantine as amazing cooks. The other half will come out with a drinking problem.