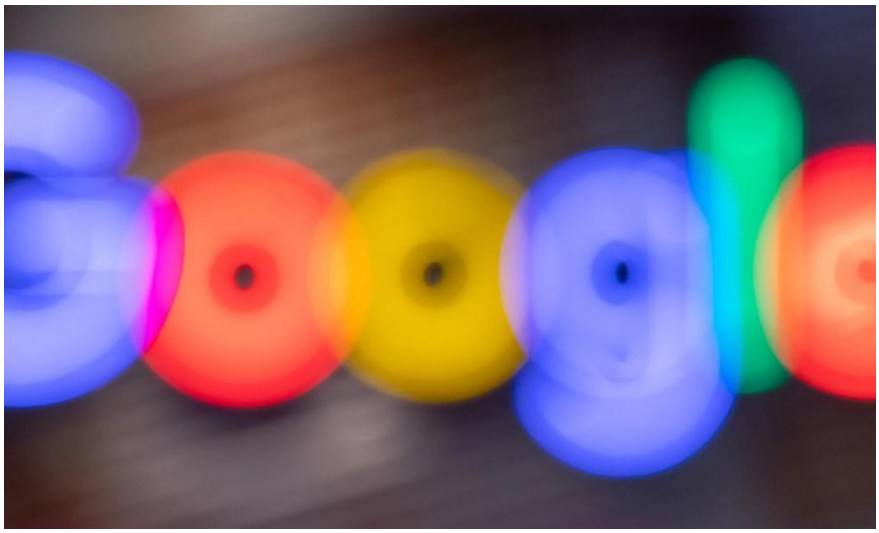
Google patched two more zero-day vulnerabilities in Chrome

In just 3 weeks, Google has fixed 5 zero-day vulnerabilities in Chrome browser. You should keep Google Chrome up to date to avoid the risk of being exploited by hackers.

Today, Google released Chrome version 86.0.4240.198 to fix two zero-day vulnerabilities that are being exploited. Thus, in just 3 weeks, Google had to patch 5 zero-day vulnerabilities on its browser. The difference is that the first 3 vulnerabilities were discovered internally, while the last 2 were reported by anonymous sources.



Google constantly has to patch the zero-day vulnerability in Chrome. Photo: ZDN

Details of the attacks exploiting the two new vulnerabilities have not been released yet. According to information from Google, these include CVE-2020-16013 and CVE-2020-16017. It is not clear whether they are used alone or in combination. The three previous vulnerabilities are CVE-2020-15999, CVE-2020-16009 and CVE-2020-16010.

The zero-day vulnerability is an unprecedented and unpatched software vulnerability. Most of these flaws are deployed in targeted attacks that target a select number of objects, so the average user should not be too concerned. Although it is unclear how dangerous the vulnerability is to regular users, Google still advises updating v86.0.4240.198 through Chrome's built-in update function.

Google Chrome is the world's leading web browser in terms of market share. According to statistics in May, Chrome accounts for 69% of the global browser market share. You should keep Google Chrome up to date to avoid the risk of being exploited by hackers.