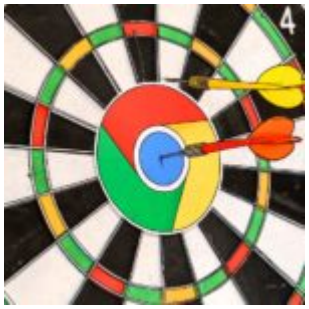
Operation WizardOpium – Kaspersky uncovers zero-day in popular web browser exploited in the wild by threat actor



Kaspersky's automated technologies have detected a new exploited vulnerability in the Google Chrome web browser. Kaspersky has allocated the vulnerability as CVE-2019-13720 and reported it to Google. A patch has been released. Upon review of the PoC provided, Google confirmed that it is a zero-day vulnerability.

Zero-day vulnerabilities are previously unknown software bugs that can be exploited by attackers to inflict serious and unexpected damage. The new exploit is used in attacks that leverage a waterhole-style injection in a Korean-language news portal. A malicious JavaScript code is inserted in the main page, which in turn, loads a profiling script from a remote site to further check if the victim's system could be infected by examining versions of the browser's user credentials. The vulnerability tries to exploit the bug through the Google Chrome browser and the script checks if version 65 or later is being used. The exploit gives an attacker a Use-After-Free (UaF) condition, which is very dangerous because it can lead to code execution scenarios.

The detected exploit was used in what Kaspersky experts call "Operation WizardOpium". Certain similarities in the code point to a possible link between this campaign and Lazarus attacks. Additionally, the profile of the targeted website is similar to what has been found in previous DarkHotel attacks, which have recently deployed comparable false flag attacks.

The exploited vulnerability was detected by Kaspersky's Exploit Prevention technology, embedded in most of the company's products.
"The finding of a new Google Chrome zero-day in the wild once again demonstrates that it is only collaboration between the security community and software developers, as well as constant investment in exploit prevention technologies, that can keep us safe from sudden and hidden strikes by threat actors," said Anton Ivanov, a security expert at Kaspersky.

Kaspersky products detect the exploit as PDM:Exploit.Win32.Generic.

Kaspersky recommends taking the following security measures:
– Install the Google patch for the new vulnerability as soon as possible.
– Make sure you update all software used in your organization on a regular basis, and whenever a new security patch is released. Security products with Vulnerability Assessment and Patch Management capabilities may help to automate these processes.
– Choose a proven security solution, such as Kaspersky Endpoint Security for Business, that is equipped with behavior-based detection capabilities for effective protection against known and unknown threats, including exploits.
– In addition to adopting essential endpoint protection, implement a corporate-grade security solution that detects advanced threats on the network level at an early stage, such as Kaspersky Anti Targeted Attack Platform.
– Make sure your security team has access to the most recent cyberthreat intelligence. Private reports on the latest developments in the threat landscape are available to Kaspersky Intelligence Reporting customers. For further details, contact: intelreports@kaspersky.com.
– Last, but not least, ensure your staff is trained to understand and implement the basics in cybersecurity hygiene.