Title:

Google Urgently Releases Security Upgrades to Address Fourth Actively Exploited Zero-Day Vulnerability in 2023

Published on September 11, 2023

By: Sai Rithwik



In a swift response to mounting cybersecurity concerns, Google has rolled out critical security updates to address an actively exploited zero-day vulnerability that has been plaguing users since the beginning of this year. The flaw, officially identified as CVE-2023-4863, marks Google's fourth such zero-day vulnerability patched in 2023. 

The zero-day flaw, which has been actively exploited in real-world attacks, was brought to Google's attention by security experts from the Apple Security Engineering and Architecture (SEAR) and The Citizen Lab at the Munk School of The University of Toronto. The incident was reported to Google on September 6, 2023.

In a statement, Google expressed gratitude to the security researchers who collaborated in the development of these urgent security upgrades, emphasizing their joint efforts in preventing security flaws from reaching the stable channel.

The zero-day vulnerability, CVE-2023-4863, specifically pertains to a significant heap buffer overflow bug found in WebP, a widely used image format. This type of vulnerability can be exploited by attackers to gain unauthorized access and execute malicious code, potentially compromising user data and system integrity.

Furthermore, Google's prompt response to this threat underscores the critical nature of zero-day vulnerabilities. They are called "zero-day" because they are exploited by malicious actors before developers become aware of them, leaving users and organizations vulnerable to attacks.



In a related development, the United States Cybersecurity and Infrastructure Security Agency (CISA) has added two more zero-day vulnerabilities, identified as CVE-2023-41064 and CVE-2023-41061, to its list of known exploited vulnerabilities. These security holes were reportedly used to deploy the infamous Pegasus spyware by the NSO Group on iPhones.

The vulnerabilities were found within the Image I/O and Wallet frameworks, posing a significant threat to Apple users. The buffer overflow vulnerability, CVE-2023-41064, was initially identified by researchers from Citizen Lab. Apple has promptly addressed this issue with improved memory management.

Users are urged to update their systems and applications as soon as possible to ensure they are protected against these vulnerabilities. The prompt action taken by Google and Apple highlights the ongoing challenges posed by zero-day vulnerabilities in the digital age and the importance of collaborative efforts in safeguarding online security.

As the threat landscape continues to evolve, users and organizations must remain vigilant, prioritize regular updates, and collaborate with security experts to mitigate the risks associated with these hidden flaws.