Serianu Cyber Security Advisory

Chrome Zero-Day Vulnerabilities

Serianu SOC Advisory Number:

TA – 2020/020

Date(s) issued:

24th November, 2020

Systems Affected

- Chrome Browser for Both Desktops and Android

OVERVIEW:

The Serianu research team is sharing this technical alert to advise IT, professionals and managers in organizations, to increase the priority on patching vulnerabilities that are increasingly being exploited by sophisticated malicious actors. This alert explains the full impact, execution and recommendation of the zero-day vulnerabilities identified in chrome browser.

About the Vulnerabilities (CVE-2020-16009, CVE-2020-16010)

Google patched 2 zero-day vulnerabilities in its Chrome browser, the third time in two weeks that the company has fixed a Chrome security flaw that's under active exploit. Zero-day vulnerability is a security flaw that is unknown to the software developers or software vendors, the vulnerability is usually exploited by cybercriminals before a patch becomes available. CVE-2020-16009 is the vulnerability present in the desktop version of the browser, CVE-2020-16010 in the mobile (Android) version.

According to our research the two flaws are :

- **CVE-2020-16009 -** An inappropriate implementation flaw in V8, Chrome's open source JavaScript engine, which is used by attackers to achieve remote code execution via a crafted HTML page. Successful exploits will allow the attacker to obtain sensitive information and execute arbitrary code in the Chrome sandbox.

- **CVE-2020-16010** - A heap-based buffer overflow vulnerability in UI on Android, which is used to escape Chrome's sandbox (escalate privileges on the vulnerable system) via a crafted HTML page. A buffer overflow occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations. Successful exploitation of the vulnerability may allow an attacker to compromise the affected system

These two zero-days come after Google also patched:

- **CVE-2020-15999** - A zero-day in Chrome's FreeType font rendering library that Google patched on October 20. This Chrome zero-day was utilized together with a Windows zero-day (**CVE-2020-17087**), which Microsoft patched yesterday.
- **CVE-2020-16009** - A second zero-day in Chrome's V8 JavaScript engine, which Google patched on November 2.
- **CVE-2020-16010** - a third zero-day in Chrome for Android, impacting the browser's user interface (UI) component.

Desktop versions of Chrome typically update automatically. That means that, for most users, patches for **CVE-2020-16009** and **CVE-2020-15999** have already been installed, as long as they've recently restarted their browser. Chrome for Android is updated through Google Play.

Recommendation:

Update your Chrome Installations

1. Serianu advices users to keep their devices, desktop or android phone browser regularly updated to mitigate risk associated with the flaw. Chrome version 86.0.4240.183 for Windows, macOS and Linux is the latest stable version that contains fixes for CVE-2020-16009 and 9 additional vulnerabilities. Users who don't have auto-updating switched on should manually check for the update.
2. Chrome v86.0.4240.185 for Android contains all the fixes plus the one for CVE-2020-16010. The update for the app is available on Google Play.
3. Chrome users are advised to look for the latest update by going to **Help** > **About Google Chrome** after clicking on the three dots button from the top-right corner of the browser window. The update is being rolled out in stages and may take some time to reach all users.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organization or individual that has access to commonly exploited vulnerabilities to share it with us through our email info@serianu.com to allow us to analyze any indicators of compromise (IOC).