The unsafe 'feature' on UC Browser allows hackers to take control of Android phones remotely

Watch! If you are constantly using UC Browser as the main browser on your smartphone, now is the time to carefully consider uninstalling it immediately.

Watch! If you are constantly using UC Browser as the main browser on your smartphone, now is the time to carefully consider uninstalling it immediately.

Why is that? Simply because this once-popular 'browser' platform is being questioned by security researchers that contains an insecure 'feature' that allows an attacker to exploit to automatically download Down and execute code on your Android device remotely.

Developed by the UCWeb team owned by Alibaba, UC Browser is one of the most popular mobile browsers in the world, especially in China and India, with a huge number of users, coming up. 500 million members worldwide.

1. Experience Microsoft Edge with Chromium, nice interface, fast loading speed, better RAM than Chrome

According to a new report published by security company Dr. Web, since 2016, UC Browser for Android has been repeatedly discovered possessing "hidden" features, allowing publishers to download new libraries and modules from their servers and install them on the user's mobile device at any time.

Vulnerability allows deploying MiTM attacks

So what's the worry about the feature that contains vulnerabilities on UC Browser? As it turned out, the researchers discovered that this feature silently downloaded many new plugins from the publisher's server via the insecure HTTP protocol instead of the encrypted HTTPS protocol, so it allowed An attacker can easily perform intermediate attacks (MiTM), and at the same time push malicious modules into targeted devices.

1. Summarizing Pwn2Own 2019: Safari, VirtualBox was "pierced" on the first day, Firefox, Edge on the second day and Tesla Model 3 "closed the window"

"Because of the fact that UC Browser works with unencrypted plugins, it will be allowed to launch malicious modules without any verification. This is meant to be true. In an MITM attack, cyber criminals will only need to retrieve the server's response from http://puds.ucweb.com/upTHER/index.xhtml?dataver=pb, then replace the link to the downloadable plugin and attribute values ??to be verified, such as the repository MD5, its size and the plugin's size, so that the browser will be able to access the malicious server to download and launch the Trojan module, "security experts said.

Besides, in the PoC video shared by the security team. Web, researchers demonstrated how they could replace a plugin to view PDF documents with malicious code using a MiTM attack, forcing the UC Browser to compile a text message. new, instead of opening the file.

"Therefore, MITM attacks can help hackers through UC Browser to spread malicious plugins that perform many different behaviors. For example, they can show phishing messages to steal. Important information such as usernames, passwords, bank card details and some other personal data, 'the researchers further explained.

1. [Video] Admire the latest images of Microsoft Edge browser on Chromium platform

UC Browser has violated the Google Play Store privacy policy

It can be seen that, with the ability to allow the owner of UCWeb to download and execute arbitrary code on a user's device without reinstalling the new version, UC Browser application has seriously violated the policy. General of Google Play Store, specifically here that this application has ignored Google's authentication servers.

"This has violated Google's general rules for each software distributed in the Android Play Store. The current policy states that applications downloaded from Google Play are not allowed to change. their own code or download any other software components from third party sources.These rules have been applied to prevent the distribution of download module trojans and launch malicious plugins. Damage, and UC Browser simply ignored that, 'explained Dr. Web experts.

1. Microsoft released the Windows Defender extension for Google Chrome and Firefox browsers to protect the device

In related news, this dangerous feature has been found by security researchers in both UC Browser and UC Browser Mini, with all versions affected including the latest version of This new browser platform was recently released.

Dr. team The Web is responsible for reporting its findings to developers of both UC Browser as well as the UC Browser Mini, but they refuse to comment on this discovery and then report it directly to Google.

At the time of writing, UC Browser and UC Browser Mini "are still available, and can be downloaded and installed from Google Play. In addition, UCWeb has not released any patches, ie UC. Browser and UC Browser Mini are still silently downloading new 3rd party components on users' Android devices, while bypassing authentication from Google Play servers, "the researchers said.

Such a feature can be abused in supply chain attacks when the company's server is compromised, allowing an attacker to push malicious updates to a large number of users. At the same time, like the way we've been seen in a recent supply chain attack, targeting ASUS has infringed on more than 1 million of its computers.

The above is the whole reason why we recommend you to consider uninstalling UC Browser immediately, or at least until UCWeb has a clear explanation and fix the problem.