UC Browser Android - lucrative bait for URL spoofing attacks

With over 600 million installations through Play Store, UC Browser and UC Browser Mini Android are one of the most used mobile browser platforms in the world.

With over 600 million installations through Play Store, UC Browser and UC Browser Mini Android are one of the most used mobile browser platforms in the world. However, this browser has been repeatedly criticized for containing serious vulnerabilities that could be exploited by hackers, causing great damage to users, and the latest version this time is not foreign. rate. UC Browser and UC Browser Mini Android (the latest version) is said to contain vulnerabilities that make it easy for users to become victims of URL spoofing attacks. This vulnerability has recently been discovered by security researcher Arif Khan and immediately reported to UC's security team.

1. A very large black web market has just been destroyed

Basically, URL spoofing attacks are conducted based on the attacker's ability to change the URL displayed in the web browser's address bar to fool the victim, making them think that the site They are accessed controlled by a trusted party. As in the case of the address bar spoofing vulnerability discovered by researcher Arif Khan in the UC Browser for Android application, the malicious website is actually controlled by the attacker.

Victims may be tricked into accessing domains controlled by an attacker and disguised as highly configurable websites. Web sites of this type will allow an attacker to steal victim's information using a redirect to a phishing landing page, or infect malware to their computer through promo campaigns. malicious report.

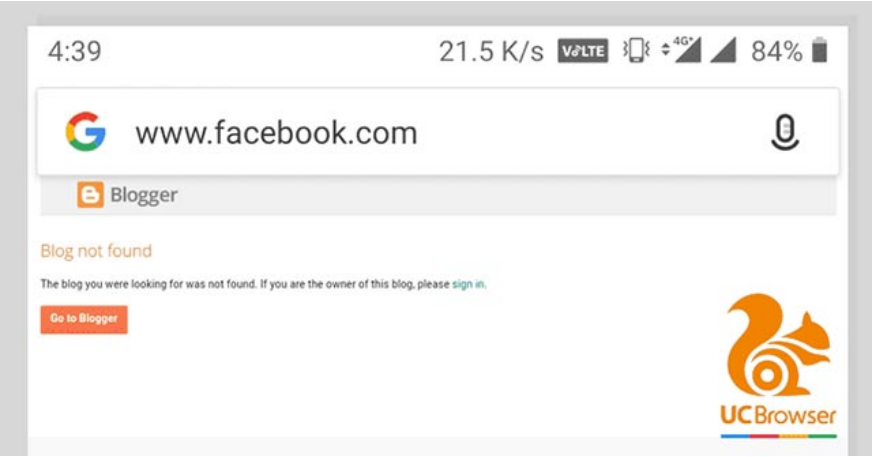
1. More than 4,000 Office 365 accounts are affected by account hijacking attacks

URL spoofing issue

"It can be said, spoofing the URL address bar is one of the most dangerous forms of phishing attacks today. Because in fact, URL address checking is the only way to identify the site that the user is. access, "explained Arif Khan.

In a recently posted security recommendation, the researcher also pointed out that the UC Browser and UC Browser Mini platforms contain vulnerabilities that allow an attacker to "set a domain name (phishing I) make the site targeted in an extremely sophisticated way, for example, a URL directed to blogspot.com address can be transformed by hackers to facebook.com just by navigating the user to the address. *www [.] google [.] com [.] blogspot.com [/? q =] www.facebook.com.*

"This form of attack can be done successfully mainly because some mobile browsers such as UC Browser and UC Browser Mini currently use bad regex checking features. In other words, some platforms Mobile browser platform is trying to improve UX (user experience) by displaying only search terms when users conduct a search for something on search engines such as Google ', Mr. Khan added.



1. Dell computers became victims of RCE attacks by vulnerabilities in SupportAssist

According to the researcher, "Basically, some browsers simply check whether the URL the user is visiting starts with the phrase *www [.] Google [.] Com* , so An attacker can take advantage of this loophole so that he can bypass the regex checking feature and thereby strip the server access and then fake the URL address bar '.

In this case, to avoid exposing users, the developers of UC Browser and UC Browser Mini should remove the "improved" features of UX, and set the browser to display the real domain name in any case "if they can't offer better regex solutions or release effective security features for this function".

During the analysis, Mr. Arif Khan noticed something quite strange, that some old UC Browser versions were completely unaffected by this attack. This indicates that one or even some of the new features added to these two browser platforms is the cause of the problem.

1. Malware stored in Google Sites sends data to the MySQL server

UCWeb ignored the fake URL report on UC browser

In addition, Mr. Arif Khan also published 2 proof videos (PoC) [UC Browser, UC Browser Mini] showing how attackers could take advantage of the fake address bar flaw to lead the victims. Potential leads to phishing landing pages or landing pages containing malicious ads.

This problem was discovered in UC Browser versions 12.11.2.1184 and UC Browser Mini 12.10.1.1192. However, at the time of writing, the developer responsible for the two applications is UCWeb, which has not yet released a patch or even public explanations for users, despite the fact that the problem This was announced by Mr. Arif Khan to UCWeb's security department in detail and extremely responsible on April 30th. Thus, nearly ten days have passed without UCWeb still having any action to solve the problem.

In particular, after Arif Khan's report was posted in UCWeb's systems, it was assigned the "Ignored" status by the company's security team!

Title	Self-Ranking	Status	Ranking	Reputation	Reward
URL Address Bar spoofing...	Important	Ignored	-	0	0

1. Malicious ad campaigns abuse Chrome to steal 500 million iOS user sessions

At the end of March, the two Android browser platforms were also pointed out by security researchers that they contain vulnerabilities that make it easy for users to become victims of intermediate attacks (MiTM). by downloading and installing a number of additional modules from UCWeb's own servers through unprotected channels and, of course, are not safe, and ignore Google Play Store servers. Shortly thereafter, even the desktop UC Browser application was discovered to contain a similar vulnerability. However, this situation is judged to be more dangerous because it could allow malicious agents to silently download malicious code extensions on users' computers.

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

We recommend that you stop using UC Browser and UC Browser Mini Android until UCWeb gives you satisfactory moves.

You finished reading the article "**UC Browser Android - lucrative bait for URL spoofing attacks**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com