Google resolves browser vulnerability, positive response wins praise

September 7 2018, by Nancy Owano

Oh, no. Never comforting to read of login thefts of any sort and it is small wonder that a security sleuth made news when he discovered an issue with Chrome. Once again, the price of convenience becomes a topic, this time in the offer to save Wi-Fi credentials and re-enter them automatically for your convenience.

A Chrome browser issue was described earlier this month which could have left a door open for hackers. The good news is that the security glitch in the popular browser was resolved; Google fixed the

vulnerability.

The problem involved credentials auto-filled on unencrypted HTTP pages. SureCloud delivered the subsequent news that the latest update of Chrome (tested against version 69.0.3497.81) addressed the issue. The latest version of the Chrome browser, version 69, has been released and it carried the patch.

ZDNet security reporter Catalin Cimpanu said it had been "a design issue" that attackers could exploit to steal the WiFi logins, whether from home or from corporate networks.

BetaNews quoted Luke Potter, SureCloud's cybersecurity practice director. "There is always a trade-off between security and convenience, but our research clearly shows that the feature in web browsers of storing login credentials is leaving millions of home and business networks wide open to attack—even if those networks are supposedly secured with a strong password."

Elliot Thompson, a researcher with UK cyber-security firm SureCloud, had put together a technique exploiting the design issue, said Cimpanu. Thompson's "Wi-Jacking" worked with Chrome on Windows.

"During a recent engagement we found an interesting interaction of browser behaviour and an accepted weakness in almost every home router that could be used to gain access a huge amount of WiFi networks," said Thompson's SureCloud post on September 4.

The browser behavior related to saved credentials. Credentials saved in a browser, tied to a URL, are automatically inserted into the same fields when seen again. The router weakness was in the use of unencrypted HTTP connections to management interfaces. Thompson, though, said there was a solution for this path to credential-theft and he discussed it in

his September 4 post.

"Fundamentally this is just a flaw in the way origins are shared and trusted between networks. In the case of home routers, they are predictable enough to be a viable target. The easiest solution would be for browsers to avoid automatically populating input fields on unsecured HTTP pages. It is understandable that this would lower usability, but it would greatly increase the barrier to credential theft."

At the time, Thompson recommended to "Clear your browser's saved passwords and don't save credentials for unsecure HTTP pages."

"Thompson says he reported the issue to Google, Microsoft, and ASUS in March, this year," said Cimpanu. "Google addressed his report by not allowing Chrome to auto-fill passwords on HTTP fields."

In addition to Chrome, are other browsers vulnerable? "Firefox, IE/Edge and Safari require significant user interaction, so attack does work, but is more of a social engineering based," said Thompson on September 4. "With Chrome it is significantly more seamless."

The usual advice applies: Update. Cimpanu wrote, "Updating to Chrome 69.0.3497.81 or later should keep users safe from Wi-Jacking attacks."

Commenting on Google's addressing the issue, Thompson said, "This is a positive response from Google and is great to see."

More information: www.surecloud.com/sc-blog/wifi … utm_content=76704482