Paul Flanagan Due: 31-Jan-2019

Recent Network Security Event

“EmPoWeb”: An Exploit of Web Applications and Browser Plug-in Privileges

Browser security researchers, headed by Dolière Francis Somé of Université Côte d’Azur in Inria, France, have recently identified a potential exploit of certain browser extensions with insufficiently robust built-in privilege security. Attackers can write web based applications that are able to use these flaws to read personal information or even store data and download files to save on a user's device. Browser extensions are often given special access privileges to users' sensitive information, such as credentials (stored as cookies), browsing history, and bookmarks. By writing malicious web applications, disguised as online forms or embedded word processing apps, attackers can exploit these permissions to gain uninhibited access to the host device at the same level reserved for browser extensions. Ordinarily, web applications are restricted by what is known as the "Same Origin Policy", which denies these apps any read and write privileges of user data across separate domains, barring the provision of express permission, typically given by the user. Browser extensions, on the other hand, are not subject to the same Policy, so that they may enhance the experience of the user, and as such many extensions are only capable of performing their goals after being given this permission. What the French researchers have found is that this policy can be bypassed via weaknesses in third party browser extensions which have been given special permissions by the user in order to function.

These offending web apps execute tailored code whose aim is to trigger certain browser extensions. Once they have been invoked, the app is able to exploit any less secure extensions currently installed for the special privileges given to them by the user and for their ability to circumvent the Same Origin Policy. At this point, the web application is free to execute more malicious code to achieve anything from accessing stored personal data to installing files onto the host system.

Using a method called privilege escalation, the application sends and receives messages with the browser extension over the “postMessage” API. Because the insecure extension fails to sanitize these messages, the application is then able to act through the extension using specially crafted messages to bypass these security flaws and interact with the private data and actions normally restricted from web applications.

Somé and his team have created a browser-compatible tool which has enabled them to test the security and weaknesses of various extensions available in a cross-browser extension store available on Chrome, Firefox, and Opera. Additionally, they have shared their findings with the owners and developers of these browsers, working with them to help find ways to fix this security flaw. In the meanwhile, many susceptible extensions have been temporarily patched or pulled from the store so that a more permanent solution can be achieved.

The implications of this flaw are numerous: in a worst case scenario, it could heavily impact the way extensions for browsers function, which have become a central aspect of the userbase’s ability to customize its internet browsing experiences. At the very least, it will mean that curators and developers of browser extensions will need to be very careful and deliberate with the permissions they require for their extensions, and intensely overhaul or totally rework existing extensions to be more secure in regards to this exploit.

Works Cited:

<https://threatpost.com/web-apps-browser-extensions-backdoors/141061/> ; written 22-Jan-2019

<https://www-sop.inria.fr/members/Doliere.Some/papers/empoweb.pdf> ; written 10-Jan-2019

<https://en.wikipedia.org/wiki/Same-origin_policy> ; last edited 26-Jan-2019