

New vulnerability in Mozilla Firefox allows third parties to access a saved password store

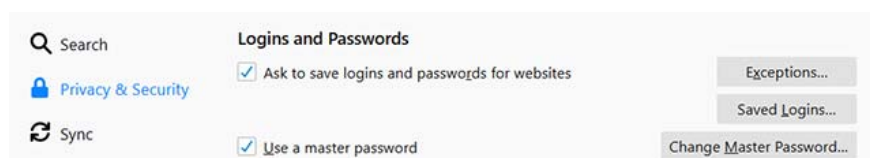
Recently, Mozilla has released version 68.0.2 for Firefox to patch a serious vulnerability that allows third parties to access and copy the password store that you have stored in your browser.

Recently, Mozilla has urgently released version 68.0.2 for Firefox to patch a serious vulnerability that allows third parties (hackers, applications, advertising providers .) to access and copy left. The password store that the user saves on the browser, specifically in this browser's Save Logins database, even when protected by another password.

"Every password stored in 'Saved Logins' can be copied without permission, without entering the master password," Mozilla Firefox's security recommendation said. At the same time this vulnerability is being monitored with the CVE-2019-11733 identifier, and the impact rating is 'moderate'.

This vulnerability is dangerous in that it allows anyone who owns local access rights to a computer running Firefox (unpatched version) to navigate to the Save Logins dialog in Options> Privacy & Security, and optionally copy the password as well as any login information stored just by right-clicking and selecting the option "Copy Password".

1. Mozilla restarted the open-source IoT platform Project Things under the name WebThings



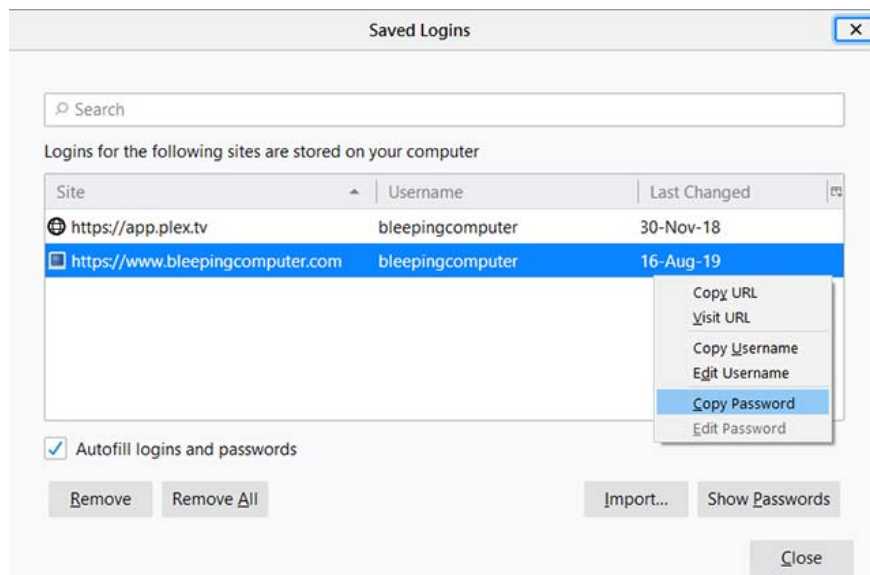
Login and Firefox password

As mentioned, Saved Logins is a repository for user login information on Firefox. Saved Logins are also protected by a separate password, called a master password. Thus, if you want to access the login information store, you will have to provide the master password. However, security experts have discovered that login information stored in Saved Logins can be copied to clipboard via the 'copy password' option in the context menu, without having to enter the previous master password. First, it facilitates the password stealer who is stored in the browser.

This is obviously a vulnerability that directly affects a security method used by Firefox to prevent unauthorized access to user login information.

The Firefox 68.0.2 security patch was released by Mozilla to fix this vulnerability, which means that third parties with local access to the browser will no longer be able to steal your password in Usually the master password has been fully set up. The current task is to check if your Firefox has been updated to the latest version.

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"



Copy the stored password in Saved Logins

One thing to note, however, is that Firefox's password manager is turned on by default to allow users to save login information more conveniently.

Basically, this is a really good idea, it helps to limit most people who have a habit of using passwords extremely dangerous, but the downside is that Firefox does not require users. must also set up a master password to protect their saved login information.

Therefore, password repositories can be accessed by anyone who has physical access to the computer, thereby leading to the risk of exposing sensitive, valuable information in local attacks. via the default configuration of the browser.

1. Mozilla is about to launch non-advertising web services, with an initial fee of \$ 5 / month

The reason this password management method is still used by Mozilla is because the chance for someone to have local access to your computer is usually much smaller than if your password could leak. After logging in to online platforms, or being hijacked through online account fraud attacks that appear 'like meals' on the internet today.

One thing to mention is that Firefox, with its built-in auto-update feature, will ensure that security patches released by Mozilla are sent to global users as soon as possible. Please enable this feature on your browser.

1. Firefox will use Windows BITS service for background updates

Firefox Updates

Keep Firefox up to date for the best performance, stability, and security.

Version 68.0.1 (64-bit) [What's new](#)

Show Update History...

Restart to update Firefox

Allow Firefox to

- Automatically install updates (recommended)
- Check for updates but let you choose to install them

ⓘ This setting will apply to all Windows accounts and Firefox profiles using this installation of Firefox.

Automatically update search engines

Enable automatic updates in Firefox

You finished reading the article "**New vulnerability in Mozilla Firefox allows third parties to access a saved password store**" 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.