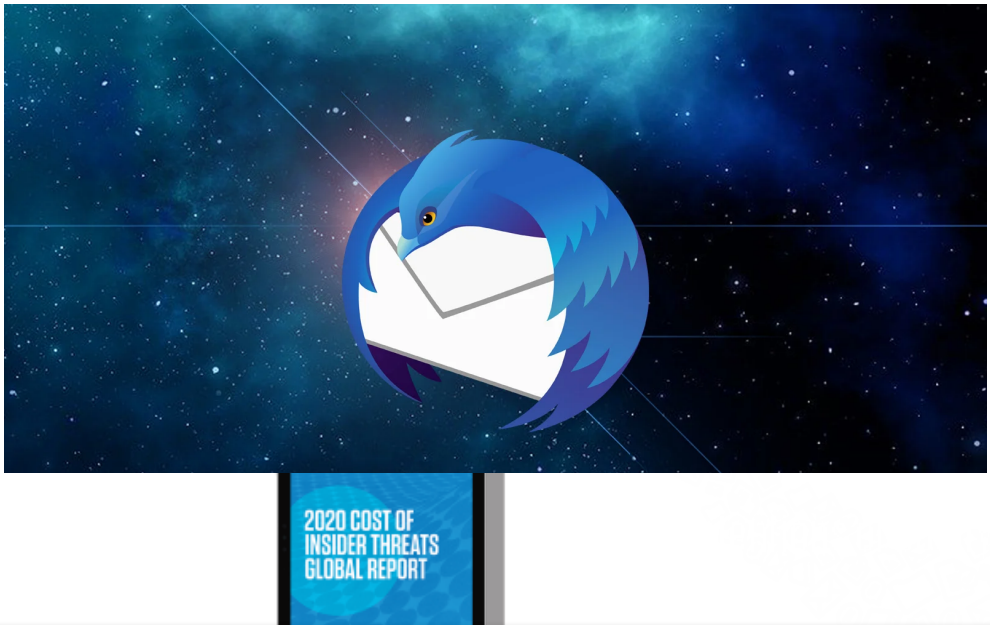
Mozilla Thunderbird 91.3 released to fix high impact flaws

By **Bill Toulas (https://www.bleepingcomputer.com/author/bill-toulas/)**

November 5, 2021 09:47 AM **2**



Mozilla released Thunderbird 91.3 to fix several high-impact vulnerabilities that can cause a denial of service, spoof the origin, bypass security policies, and allow arbitrary code execution.

Triggering most of the newly discovered bugs requires a user to open a specially crafted website in a browsing context, so the exploitation is relatively simple.

Multiple high-severity flaws

Mozilla Thunderbird 91.3 fixes ten flaws discovered by various researchers (https://www.mozilla.org/en-US/security/advisories/mfsa2021-50/) that cover a broad spectrum of the email client's functionality.

- CVE-2021-38503: iframe bypass restrictions that allow script execution
- CVE-2021-38504: user-after-free in the file picker dialog, leading to memory corruption and a potentially exploitable crash
- CVE-2021-38505: Windows 10 Cloud Clipboard sensitive data recording, copying sensitive user data to the user's Microsoft account, increasing the risk of information disclosure.
- CVE-2021-38506: Forcing Thunderbird to go into fullscreen mode without user interaction, laying the ground for UI spoofing and phishing attacks.
- CVE-2021-38507: Bypass the 'Same-Origin-Policy' by exploiting the Opportunistic Encryption feature.
- CVE-2021-38508: Ability to overlay the Permission Prompt to trick

- CVE-2021-38509: Spoof the JavaScript alert () dialog with arbitrary contents.
- CVE-2021-38510: Bypass 'Download Protections' on .inetloc files, allowing code execution on macOS.
- MOZ-2021-0008: Use-after-free in HTTP2 Session object, leading to memory corruption and possibly to an exploitable crash.
- MOZ-2021-0007: Memory corruption flaws that may lead to arbitrary code execution.

One vulnerability tracked as CVE-2021-38505 is of particular interest as its related to the Windows 10 Cloud Clipboard.

The Windows 10 Cloud Clipboard feature was introduced in 2018, and if enabled, will sync data you copy to the clipboard into the cloud, so it is available on other devices you have an account.

To prevent sensitive data from being synced to the cloud, Microsoft introduced specific clipboard formats that Windows would not copy to the cloud. However, Thunderbird and Mozilla did not use those formats, potentially allowing sensitive data to be synchronized.

"Microsoft introduced a new feature in Windows 10 known as Cloud Clipboard which, if enabled, will record data copied to the clipboard to the cloud, and make it available on other computers in certain scenarios," explained Mozilla.

"Applications that wish to prevent copied data from being recorded in Cloud History must use specific clipboard formats; and Firefox before versions 94 and ESR 91.3 did not implement them. This could have caused sensitive data to be recorded to a user's Microsoft account."

Due to the severity of the above flaws, upgrading the popular email client to version 91.3 or later should be done as soon as possible.

To upgrade to the latest version immediately, open Thunderbird, click on the app menu, and select **Help** > **About Thunderbird**. From there, you will be offered the option to download and install the latest available version.

Ubuntu has also released a security notice (https://ubuntu.com/security/notices/USN-5132-1) for Thunderbird for the flaws that concern the Linux distribution, and an updated package has been made available on the stable repository.

Upgrade to 91.x lagging

The latest stats from Mozilla show that only 65% (https://stats.thunderbird.net/#version) of Thunderbird users have upgraded to 91.x, with the rest still using older, unsupported, and now vulnerable versions.

A month ago, Mozilla forced an upgrade (https://www.bleepingcomputer.com/news/software/mozilla-upgrades-older-thunderbird-clients-to-the-latest-version/) from 78.x to 91.x, to ensure that everyone is running the latest stable version of the email client.

However, due to add-on incompatibility issues between the two major releases, many users have opted to stay on 78.x, which from a security perspective, is getting increasingly risky.

Related Articles:

Mozilla upgrades older Thunderbird clients to the latest version (https://www.bleepingcomputer.com/news/software/mozilla-upgrades-older-thunderbird-clients-to-the-latest-version/)

Android October patch fixes three critical bugs, 41 flaws in total (https://www.bleepingcomputer.com/news/security/android-october-patch-fixes-three-critical-bugs-41-flaws-in-total/)

Over 30,000 GitLab servers still unpatched against critical bug (https://www.bleepingcomputer.com/news/security/over-30-000-gitlab-servers-still-unpatched-against-critical-bug/)

Android November patch fixes actively exploited kernel bug (https://www.bleepingcomputer.com/news/security/android-november-patch-fixes-actively-exploited-kernel-bug/)

Mozilla blocks malicious add-ons installed by 455K Firefox users (https://www.bleepingcomputer.com/news/security/mozilla-blocks-malicious-add-ons-installed-by-455k-firefox-users/)