



**THREAT ADVISORY**



**VULNERABILITY  
REPORT**

**Mozilla addresses security vulnerabilities in  
Firefox, Firefox ESR, and Thunderbird**

Date of Publication

2 June 2022

Admiralty code

A1







TA Number

TA2022110

# Summary

Mozilla has released updates that address up to eight high severity vulnerabilities (as per Mozilla) in Firefox, Firefox ESR, and Thunderbird. These vulnerabilities could allow an attacker to exploit the system and take control, allowing an attacker to install applications, edit or damage data as well as create new accounts with full user rights. These vulnerabilities can allow remote code execution on successful exploitation if countermeasures are not taken.

## CVEs

CVE	NAME	PATCH
CVE-2022-31736	Cross-Origin resource's length leaked	
CVE-2022-31737	Heap buffer overflow in WebGL	
CVE-2022-31738	Browser window spoof using fullscreen mode	
CVE-2022-31739	Attacker-influenced path traversal when saving downloaded files	
CVE-2022-31740	Register allocation problem in WASM on arm64	
CVE-2022-31741	Uninitialized variable leads to invalid memory read	

CVE	NAME	PATCH
CVE-2022-31747	Memory safety bugs in Firefox	✓
CVE-2022-31748	Memory safety bugs fixed in Firefox	✓
CVE-2022-1834	Braille space character caused incorrect sender email to be shown for a digitally signed email	✓

# Technical Details

## #1

There are **several** security vulnerabilities that have been fixed across FireFox, Firefox ESR and Thunderbird. **CVE-2022-31737** allows a **malicious webpage** to cause an out-of-bounds write in WebGL, which can lead to **memory corruption** and **exploitable crash** across all these versions. **CVE-2022-31741**, **CVE-2022-31747** and **CVE-2022-31748** have shown evidence of memory corruption and we can presume that some of these could be exploited to run arbitrary code.

## #2

Another vulnerability **CVE-2022-1834** was addressed in Thunderbird 91.0, where the attacker could exploit the **Braille Pattern Blank space character** by sending an email message with an attacker's digital signature being invisible due to the following Braille spaces, thus leading to Thunderbird approving of **invalid digital signatures**, and causing potentially exploitable crashes.

## #3

Other vulnerabilities such as **CVE-2022-31738** where the iframe could disrupt the browser and result in **potential user confusion** or **spoofing attacks** if the necessary updates are not made to the three versions.

# Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-31736	Mozilla Thunderbird: 91.0 - 91.9.1	• <u>cpe:2.3:a:mozilla:m ozilla_thunderbird:9 1.9.1:*.~*~*~*~*~*~*</u>	CWE-200
CVE-2022-31737	Mozilla Firefox: 90.0 -		CWE-787
CVE-2022-31738	100.0.2		CWE-451
CVE-2022-31739	Firefox ESR: 91.0 -		CWE-22
CVE-2022-31740	91.9.1		CWE-119
CVE-2022-31741			CWE-457
CVE-2022-31747			CWE-119
CVE-2022-1834			CWE-451
CVE-2022-31748	Mozilla Firefox: 90.0 - 100.0.2 Firefox ESR: 91.0 - 91.9.1	• <u>cpe:2.3:a:mozilla:m ozilla_firefox:100.0.2 .~*~*~*~*~*~*</u>	CWE-200

## Patch Links

<https://www.mozilla.org/en-US/firefox/all/#product-desktop-release>

## References

<https://www.mozilla.org/en-US/security/advisories/mfsa2022-20/#CVE-2022-31736>

<https://www.mozilla.org/en-US/security/advisories/mfsa2022-21/>

<https://www.mozilla.org/en-US/security/advisories/mfsa2022-22/>



# What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.



At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

**2 June 2022 • 3:00 PM**

© 2022 All Rights are Reserved by HivePro



More at [www.hivepro.com](http://www.hivepro.com)