An Lárionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC Advisory

Security Vulnerability fixed in Firefox, Firefox ESR and Thunderbird (CVE-2024-9680)

22nd, October 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP-CLEAR** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Subject to standard copyright rules, **TLP-CLEAR** information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

An Roinn Comhshaoil,
Aeráide agus Cumarsáide
Department of the Environment,
Climate and Communications

Description

CVE ID: CVE-2024-9680

Published: 2024-10-09

Vendor: Mozilla

Product: Firefox, Firefox ESR and Thunderbird

CVSS3.0 Score: 9.8

Summary: Mozilla has disclosed a vulnerability that affects it's Firefox, Firefox ESR and Thunderbird products.

CVE-2024-9680 refers to a critical, actively exploited "Use-After-Free" vulnerability in the animation timeline component of Mozilla's web developer tools, which has the potential to lead to arbitrary code being executed.

Mozilla has disclosed that they have had reports of this vulnerability being exploited in the wild.

Products affected

- Firefox versions prior to **131.0.2**
- Firefox ESR versions prior to **128.3.1**
- Firefox ESR versions prior to **115.16.1**
- Thunderbird versions prior to **131.0.1**
- Thunderbird versions prior to **128.3.1**
- Thunderbird versions prior to **115.16.0**
- Other Firefox (Gecko) based browsers are also affected, such as **Tor Browser**

Impact

A remote attacker could use this vulnerability to download additional malicious code, such as ransomware from another remote location, and execute it on a user's host. Successful exploitation only requires a user to visit an attacker-controlled web page, with no further user interaction.

Common Weakness Enumeration (CWE): CWE-416

Known Exploited Vulnerability (KEV) catalog: Yes

Used by Ransomware Operators: Known

Recommendations

The NCSC strongly advises affected organisations to review the latest release notes and install the relevant updates from Mozilla for the affected product.

More information can be found here:

- https://www.mozilla.org/security/advisories/mfsa2024-51/
- https://www.mozilla.org/security/advisories/mfsa2024-52/