Hive Pro

THREAT ADVISORY

Two actively exploited Zero-Day vulnerabilities discovered in Mozilla Firefox

TA2022047

Threat Level RED

Publish Date – March 7, 2022

Two critical zero-day vulnerabilities have been identified in Mozilla Firefox that are being exploited in-the-wild and tracked as CVE-2022-26485 and CVE-2022-26485. Both are use-after-free bugs that exist in XSLT parameter processing and the WebGPU IPC Framework, respectively. Attackers can exploit these flaws to cause the sandbox escape or execute arbitrary code on the affected machine.

Several controls have been introduced in recent browsers that make exploitation of these Use-after-free vulnerabilities much harder but despite this, they still seem to persist. This is a weakness related to the incorrect use of dynamic memory during program operation. Successful exploitation of this issue may lead to data corruption, program crash or arbitrary code execution.

These vulnerabilities have been fixed in versions Firefox 97.0.2, Thunderbird 91.6.2 and Firefox ESR 91.6.1

Potential MITRE ATT&CK TTPs are:
TA0001: Initial Access
TA0040: Impact
TA0004: Privilege Escalation
T1068: Exploitation for Privilege Escalation
T1499: Endpoint Denial of Service
T1189: Drive-by Compromise
T1190: Exploit-public facing application

Vulnerability Detail

CVE ID	Affected Version	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-26485	Firefox versions before 97.0.2, Thunderbird before 91.6.2, and Firefox ESR versions before 91.6.1	cpe:2.3:a:mozilla:firefox:-:*:*:*:*:*:*:* , cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:* , cpe:2.3:a:mozilla:thunderbird:*:*:*:*:*:*:*:*	Use-after-free in XSLT parameter processing	CWE-416
CVE-2022-26486			Use-after-free in WebGPU IPC Framework	CWE-416

Patch Link

https://cdn.stubdownloader.services.mozilla.com/builds/firefox-stub/en-US/win/bb09da6defac4081f06e02ac17730b9b6f1e13db4315d371a03b167a2f4b3155/Firefox%20Installer.exe

References

https://www.mozilla.org/en-US/security/advisories/mfsa2022-09/#CVE-2022-26485