**GOVERNMENT OF THE REPUBLIC OF VANUATU**

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS
& DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

**GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU**

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE
COMMUNICATION ET DE
TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

9 October 2025

**Advisory 106: Mozilla Multiple Products Remote Code Execution Vulnerability**

**Release Date:** 06th of October 2025
**Impact:** HIGH / CRITICAL
**TLP:** CLEAR

The Department of Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

## What is it?

**CVE-2010-3765** is a **remote code execution** vulnerability in Mozilla products (Firefox / SeaMonkey / Thunderbird) caused by a heap buffer overflow when mixing *document.write* and DOM insertion; it was actively exploited in October–November 2010.

## What are the Systems affected?

Affected:

- Firefox **3.5.x** through **3.5.14** and **3.6.x** through **3.6.11** — fixed in **Firefox 3.5.15** and **3.6.12**.
- SeaMonkey fixed in **2.0.10**.
- Thunderbird fixed in **3.0.10** and **3.1.6**.
(Any installs still running the pre-fixed releases are vulnerable.)

# What does this mean?

Remote, client-side: malicious JavaScript on a webpage (or web-like content in RSS/add-ons where JS is enabled) leverages incorrect index tracking in `nsCSSFrameConstructor::ContentAppended` plus `appendChild/document.write` interactions to trigger heap corruption, then downloads and executes payloads (Belmoo / Backdoor in observed incidents). Exploits were delivered via malicious pages and exploit kits in the wild.

This allows remote attackers to execute arbitrary code via vectors related to nsCSSFrameConstructor::ContentAppended. This then triggers memory corruption, as exploited in the wild in October 2010.

# Mitigation process

CERTVU recommend:

1. Patch immediately – Upgrade to the fixed product releases for affected products.
2. If for some reason the endpoint(s) cannot be updated, disable JavaScript for untrusted content, block untrusted sites via proxy/URL Filtering, and restrict RSS/add-ons that execute web content.
3. Harden endpoint by keeping AV/EDR signatures up to date.

# Reference

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2010-3765
3. https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Exploit:JS/CVE-2010-3765