# CVE Detail – CVE-2020-6819

Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.56775

## CVSS Scoring

CVSS v3.1 Score: 8.1

Severity: HIGH

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
* CWE-416: Use After Free

## CAPEC(s)

* CAPEC-26: Leveraging Race Conditions
* CAPEC-29: Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions

## Affected Products

* cpe:2.3:a:mozilla:firefox:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:firefox\_esr:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:mozilla:thunderbird:\*:\*:\*:\*:\*:\*:\*:\*