Talos Vulnerability Report

TALOS-2021-1307

Foxit Reader FileAttachment annotation use-after-free vulnerability redux

JULY 27, 2021

CVE NUMBER

CVE-2021-21870

Summary

A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 10.1.4.37651. A specially crafted PDF document can trigger the reuse of previously free memory, which can lead to arbitrary code execution. An attacker needs to trick the user into opening a malicious file or site to trigger this vulnerability if the browser plugin extension is enabled.

Tested Versions

Foxit Reader 10.1.4.37651

Product URLs

https://www.foxitsoftware.com/pdf-reader/

CVSSv3 Score

8.8 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CWE

CWE-416 - Use After Free

Details

Foxit PDF Reader is one of the most popular PDF document readers and has a large user base. It aims to have feature parity with Adobe's Acrobat Reader. As a complete and feature-rich PDF reader, it supports JavaScript for interactive documents and dynamic forms. JavaScript support poses an additional attack surface. Foxit Reader uses the V8 JavaScript engine.

We have previously disclosed this vulnerability to Foxit as being present in Foxit Reader version 10.1.3.37598. The vulnerability was tracked as TALOS-2021-1287 and was assigned CVE-2021-21822. Release notes for Foxit Reader version 10.1.4.37651 purport that this vulnerability was fixed but a closer examination and testing reveals that not to be the case. The details of the vulnerability, as well as the proof of concept PDF document demonstrating it, is the same as in our previously published advisory.

Timeline

2021-05-26 - Vendor Disclosure

2021-07-76 - Public Release

CREDIT

Discovered by Aleksandar Nikolic of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT
TALOS-2021-1336

NEXT REPORT
TALOS-2021-1345