



ADVISORY DETAILS

May 1st, 2023

Foxit PDF Reader exportXFADData Exposed Dangerous Method Remote Code Execution Vulnerability

ZDI-23-491

ZDI-CAN-19697

CVE ID [CVE-2023-27363](#)

CVSS SCORE 7.8, [AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H](#)

AFFECTED VENDORS [Foxit](#)

AFFECTED PRODUCTS PDF Reader

VULNERABILITY DETAILS This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

The specific flaw exists within the exportXFADData method. The application exposes a JavaScript interface that allows writing



ADDITIONAL DETAILS

Foxit has issued an update to correct this vulnerability. More details can be found at:

<https://www.foxit.com/support/security-bulletins.html>

DISCLOSURE TIMELINE

2023-01-20 - Vulnerability reported to vendor

2023-05-01 - Coordinated public release of advisory

CREDIT

Andrea Micalizzi aka rgod

[< BACK TO ADVISORIES](#)

General Inquiries

zdi@trendmicro.com

Find us on X

[@thezdi](#)

Find us on Mastodon

[Mastodon](#)

Media Inquiries

media_relations@trendmicro.com

Sensitive Email Communications

[PGP Key](#)



WHO WE ARE

- [Our Mission](#)
- [Trend Micro](#)
- [TippingPoint IPS](#)

HOW IT WORKS

- [Process](#)
- [Researcher Rewards](#)
- [FAQS](#)
- [Privacy](#)

ADVISORIES

- [Published Advisories](#)
- [Upcoming Advisories](#)
- [RSS Feeds](#)

BLOG

