TARLOGIC
CYBERSECURITY EXPERTS

Home / Blog / CVE-2023-27363: Proof of concept for remote code execution in Foxit Reader

# CVE-2023-27363: Proof of concept for remote code execution in Foxit Reader

15 - May - 2023 - S.T.A².R.S Team



Following the initial announcement of a critical vulnerability (**CVE-2023-27363**) which allows remote code execution in **Foxit Reader**, a functional proof-of-concept has recently been released that shows the exploitation of the vulnerability through the creation of a specially crafted PDF document.

The following GIF published on Github shows the PoC execution:
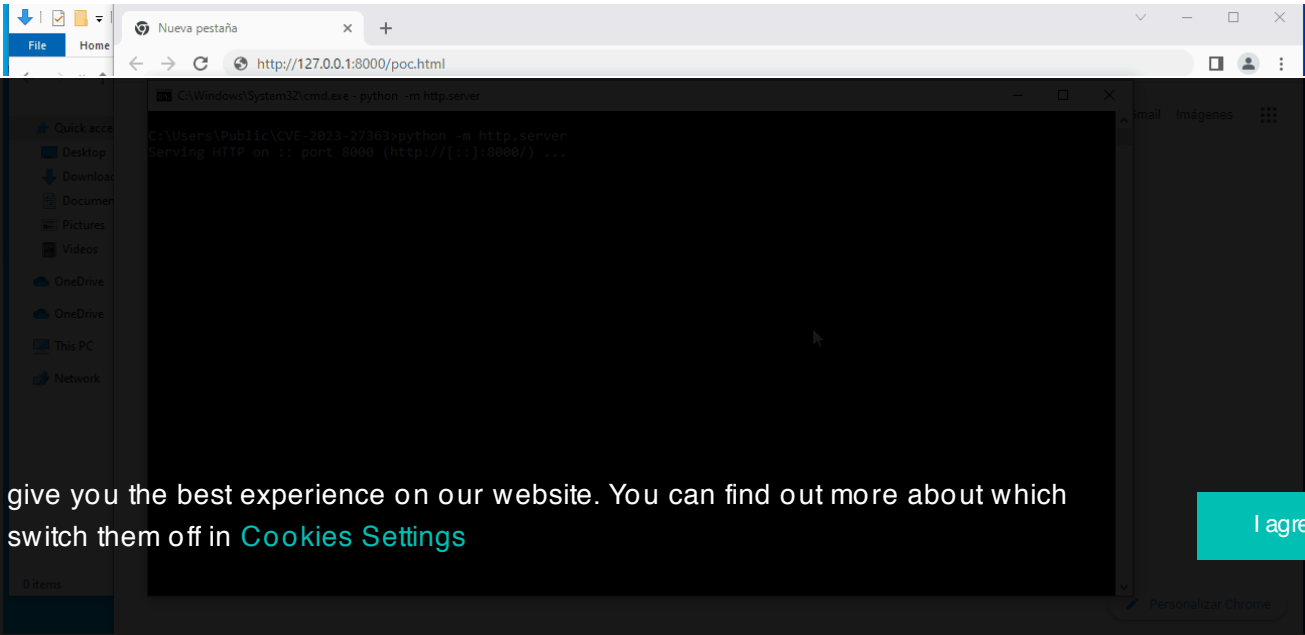


We are using cookies to give you the best experience on our website. You can find out more about which cookies we are using or switch them off in Cookies Settings

I agree

**Foxit Reader** is a free popular PDF document reader that is widely used, and is often chosen as an alternative to Adobe's PDF document reader.

The **vulnerability CVE-2023-27363**, which was initially reported by the researcher Andrea Micalizzi, exploits a problem in the handling of certain JavaScript code when validating the

Contact us now

cPath parameter in the exportXFAData method.

This situation allows arbitrary writing of files in the system in the context of the users permissions, which can be exploited to perform a code execution attack by creating a file with an .hta extension in the ASEP (AutoStart Entry Point) "StartUp folder" located in the path C:\Users\[Username]AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\.

Taking advantage of this technique, it's possible to execute arbitrary code when the affected user logs in again or after a reboot of the system.

Although the vulnerability **CVE-2023-27363** was initially announced on 2 May 2023, on 12 May a proof of concept was made public in the Github repository showing the execution of arbitrary code through the opening of a PDF document with the affected versions of Foxit Reader.

## CVE-2023-27363 main characteristics

The main characteristics of the **CVE-2023-27363 vulnerability** are detailed below:

- **CVE identifier**: CVE-2023-27363
- **Published date**: 02/05/2023
- **Affected software**: Foxit PDF Reader
- **CVSS Score**: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (9.8 Critical)
- **Affected version:** 12.1.1.15289 and earlier.

## Mitigation

The main solution is to urgently **update the Foxit PDF Reader software** to the new versions available which fix this vulnerability. These versions are available via the Foxit official website:

Foxit PDF Reader 12.1.2 update.

Foxit released an advisory with official information and **possible updates regarding this vulnerability**.

---

Share this article

Facebook - Twitter - Linkedin

Related Posts

CVE-2024-3400: Unauthenticated code injection in PAN-OS

24 - APRIL - 2024 S.T.A².R.S TEAM

Bluetooth vulnerabilities in smart locks

29 - SEPTEMBER - 2023 FRAN ÁLVAREZ WIC

Exploiting Word: CVE-2017-11826

11 - DECEMBER - 20...

Contact us now

Read more  ›

Read more  ›

Read more  ›

# Vulnerability management services

Our focus is on constant surveillance of your tech infrastructure's safety and weak points.

Vulnerability management services

**TARLOGIC**
CYBERSECURITY EXPERTS

## BUSINESS UNITS

CYBERSECURITY

CYBER INTELLIGENCE

BLACKARROW

## CONTACT INFO

EUROPE HQ:
Madrid
Quintanavides 13-23,
Business Park Vía Norte 2nd building,
Las Tablas, 28050

(+34) 912 919 319

contact@tarlogic.com

## LINKS

CYBERSECURITY PRODUCTS

CYBERSECURITY CAREERS

CYBERSECURITY GLOSSARY

TARLOGIC NEWS

CYBERSECURITY COMPANY (ABOUT US)

BSAM BLUETOOTH SECURITY METHODOLOGY

SECTORS

PARTNER CHANNEL

Privacy policy - Legal notice - Management policy - Cookies policy - Whistle-blower channel

Contact us now  💬