Security bulletins

A prompt response to software defects and security vulnerabilities has been, and will continue to be, a top priority for everyone here at Foxit Software. Even though threats are a fact of life, we are proud to support the most robust PDF solutions on the market. Here is information on some enhancements that make our software even more robust.

Please click here (/support/report-security-vulnerabilities.html) to report a potential security vulnerability.

Please click here (/support/security-advisories.html) to check security advisories.

Get notified of Foxit PDF Editor (/pdf-editor/) releases and security bulletins

youremail@mail.com Subscribe

2026

Security updates available in Foxit PDF Reader 2026.1 and Foxit PDF Editor 2026.1

Release date: March 31, 2026

Summary

Foxit has released Foxit PDF Reader 2026.1 and Foxit PDF Editor 2026.1, which address potential security and stability issues.

Affected versions

Product	Affected versions	Platform
Foxit PDF Reader (previously named Foxit Reader)	2025.3.0.35737 and earlier	Windows
Foxit PDF Editor (previously named Foxit PhantomPDF)	2025.3.0.35737 and all previous 2025.x versions, 2024.4.1.27687 and all previous 2024.x versions, 2023.3.0.23028 and all previous 2023.x versions, 14.0.2.33402 and all previous 14.x version, 13.2.2.24014 and earlier	Windows

Solution

Update your applications to the latest versions by following one of the methods below.

- In Foxit PDF Reader or Foxit PDF Editor, click on “Help” > “About Foxit PDF Reader” or “About Foxit PDF Editor” > “Check for Update” to update to the latest version.
- Click here (/products/catalog/?open=trial-foxit-pdf-reader) to download the updated version of Foxit PDF Reader from our website.
- Click here (/products/catalog/) to download the updated version of Foxit PDF Editor from our website.

Vulnerability details

Brief	Vulnerability ID	Vulnerability Category	Vulnerability Impact	Severity	CVSS Score
Addressed potential issues where the application could be exposed to an Information Disclosure vulnerability when redacting, encrypting, or printing certain PDFs embedded with specific JavaScript or document/print actions, which attackers could exploit to expose sensitive information to unauthorized actors. This occurs as the existing redaction, encryption, and printing logic does not fully cover the script-driven updates, resulting in certain content remaining unremoved/unencrypted or visible in the printed output.	CVE-2026-3774	Exposure of Sensitive Information to an Unauthorized Actor (CWE-200)	Information Disclosure	Moderate	4.7: AV:L/ /PR:N /S:U/(N/A:N

Addressed potential issues where the application could be exposed to an Uncontrolled Search Path Privilege Escalation vulnerability during installation or update checks, which attackers could exploit to execute arbitrary code by placing a malicious library or binary in a directory. This occurs as the application loads certain system libraries or resolves system executables and DLLs from an untrusted search path that can include user-writable directories.	CVE-2026-3775	DLL Hijacking (CWE-427)	Potential Arbitrary Code Execution	Important	7.8: AV:L/ PR:L/ S:U/C H/A:H
	CVE-2026-3780	Untrusted Search Path (CWE-426)	Potential Arbitrary Code Execution	Important	7.3: AV:L/ PR:L/ S:U/C H/A:H
Addressed a potential issue where the application could be exposed to a Null Pointer Dereference vulnerability and crash when opening certain PDFs that contain a stamp annotation missing the appearance (AP) entry, which attackers could exploit to launch a Denial of Service attack. This occurs as the application fails to validate the presence of the required appearance (AP) data before accessing stamp annotation resources and continues to dereference the associated objects without performing a prior null or validity check.	CVE-2026-3776	NULL Pointer Dereference (CWE-476)	Denial of Service	Moderate	5.5: AV:L/ PR:N/ S:U/C N/A:H

Addressed potential issues where the application could be exposed to a Use-After-Free vulnerability and crash when handling certain documents that contain JavaScript, which attackers could exploit to execute arbitrary code. This occurs due to the use of objects that have been deleted, destroyed, or re-created without proper validation.	CVE-2026-3777	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Moderate	5.5: AV:L/ PR:N/ S:U/C N/A:H
	CVE-2026-3779	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Important	7.8: AV:L/ PR:N/ S:U/C H/A:H
Addressed a potential issue where the application could be exposed to an Uncontrolled Recursion vulnerability and crash when handling certain PDFs with cyclic references between objects, which attackers could exploit to cause a stack overflow. This occurs as the application fails to detect or guard against cyclic references when passing the current document as a request object into APIs.	CVE-2026-3778	Uncontrolled Recursion (CWE-674)	Stack Overflow	Moderate	6.2: AV:L/ PR:N/ /S:U/C N/A:H

For more information, please contact the Foxit Security Response Team at security-ml@foxit.com (mailto:security-ml@foxit.com).

Security updates available in Foxit PDF Editor 14.0.3

Release date: March 31, 2026

Platform: Windows

Summary

Foxit has released Foxit PDF Editor 14.0.3, which address potential security and stability issues.

Affected versions

Product	Affected versions	Platform
Foxit PDF Editor (previously named Foxit PhantomPDF)	14.0.2.33402 and all previous 14.x version, 13.2.2.24014 and earlier	Windows

Solution

Update your applications to the latest versions by following one of the methods below.

- In Foxit PDF Editor, click on “Help” > “About Foxit PDF Editor” > “Check for Update” to update to the latest version.
- Click here (/products/catalog/) to download the updated version of Foxit PDF Editor from our website.

Vulnerability details

Brief	Vulnerability ID	Vulnerability Category	Vulnerability Impact	Severity	CVSS 3.0 Score	Ac
Addressed potential issues where the application could be exposed to an Uncontrolled Search Path Privilege Escalation vulnerability during installation, which attackers could exploit to execute arbitrary code by placing a malicious binary in a directory. This occurs as the application resolves system executables and DLLs from an untrusted search path that can include user-writable directories.	CVE-2026-3780	Untrusted Search Path (CWE-426)	Potential Arbitrary Code Execution	Important	7.3: AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H	•

Addressed a potential issue where the application could be exposed to a Null Pointer Dereference vulnerability and crash when opening certain PDFs that contain a stamp annotation missing the appearance (AP) entry, which attackers could exploit to launch a Denial of Service attack. This occurs as the application fails to validate the presence of the required appearance (AP) data before accessing stamp annotation resources and continues to dereference the associated objects without performing a prior null or validity check.	CVE-2026-3776	NULL Pointer Dereference (CWE-476)	Denial of Service	Moderate	5.5: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	•

Addressed potential issues where the application could be exposed to a Use-After-Free vulnerability and crash when handling certain documents that contain JavaScript, which attackers could exploit to execute arbitrary code. This occurs due to the use of objects that have been deleted, destroyed, or re-created without proper validation.	CVE-2026-3777	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Moderate	5.5: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	•
	CVE-2026-3779	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Important	7.8: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	•

Addressed a potential issue where the application could be exposed to an Uncontrolled Recursion vulnerability and crash when handling certain PDFs with cyclic references between objects, which attackers could exploit to cause a stack overflow. This occurs as the application fails to detect or guard against cyclic references when passing the current document as a request object into APIs.	CVE-2026-3778	Uncontrolled Recursion (CWE-674)	Stack Overflow	Moderate	6.2: AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	•

For more information, please contact the Foxit Security Response Team at security-ml@foxit.com (mailto:security-ml@foxit.com).

Security updates available in Foxit PDF Editor 13.2.3

Release date: March 31, 2026

Platform: Windows

Summary

Foxit has released Foxit PDF Editor 13.2.3, which address potential security and stability issues.

Affected versions

Product	Affected versions	Platform
Foxit PDF Editor (previously named Foxit PhantomPDF)	13.2.2.24014 and earlier	Windows

Solution

Update your applications to the latest versions by following one of the methods below.

- In Foxit PDF Editor, click on “Help” > “About Foxit PDF Editor” > “Check for Update” to update to the latest version.
- Click here (/products/catalog/) to download the updated version of Foxit PDF Editor from our website.

Vulnerability details

Brief	Vulnerability ID	Vulnerability Category	Vulnerability Impact	Severity	CVSS 3.0 Score	Ac

Addressed a potential issue where the application could be exposed to a Null Pointer Dereference vulnerability and crash when opening certain PDFs that contain a stamp annotation missing the appearance (AP) entry, which attackers could exploit to launch a Denial of Service attack. This occurs as the application fails to validate the presence of the required appearance (AP) data before accessing stamp annotation resources and continues to dereference the associated objects without performing a prior null or validity check.	CVE-2026-3776	NULL Pointer Dereference (CWE-476)	Denial of Service	Moderate	5.5: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	•

Addressed potential issues where the application could be exposed to a Use-After-Free vulnerability and crash when handling certain documents that contain JavaScript, which attackers could exploit to execute arbitrary code. This occurs due to the use of objects that have been deleted, destroyed, or re-created without proper validation.	CVE-2026-3777	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Moderate	5.5: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	•
	CVE-2026-3779	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Important	7.8: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	•

Addressed a potential issue where the application could be exposed to an Uncontrolled Recursion vulnerability and crash when handling certain PDFs with cyclic references between objects, which attackers could exploit to cause a stack overflow. This occurs as the application fails to detect or guard against cyclic references when passing the current document as a request object into APIs.	CVE-2026-3778	Uncontrolled Recursion (CWE-674)	Stack Overflow	Moderate	6.2: AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	•

For more information, please contact the Foxit Security Response Team at security-ml@foxit.com (mailto:security-ml@foxit.com).

Security updates available in Foxit PDF Editor for Mac 2026.1/14.0.3/13.2.3 and Foxit PDF Reader for Mac 2026.1

Release date: March 31, 2026

Platform: macOS

Summary

Foxit has released Foxit PDF Editor for Mac 2026.1/14.0.3/13.2.3 and Foxit PDF Reader for Mac 2026.1, which address potential security and stability issues.

Affected versions

Product	Affected versions	Platform
Foxit PDF Editor for Mac (previously named Foxit PhantomPDF *Mac*)	2025.3.0.69570 and all previous 2025.x versions, 2024.4.1.66479 and all previous 2024.x versions, 2023.3.0.63083 and all previous 2023.x versions, 14.0.2.69164 and all previous 14.x versions, 13.2.2.63349 and earlier	macOS
Foxit PDF Reader for Mac (previously named Foxit Reader *Mac*)	2025.3.0.69570 and earlier	macOS

Solution

Update your applications to the latest versions by following one of the methods below.

- In Foxit PDF Reader for Mac or Foxit PDF Editor for Mac, click on “Help” > “About Foxit PDF Reader” or “About Foxit PDF Editor” > “Check for Update” to update to the latest version.
- Click here (/products/catalog/?open=trial-foxit-pdf-reader) to download the updated version of Foxit PDF Reader for Mac from our website.
- Click here (/products/catalog/) to download the updated version of Foxit PDF Editor for Mac from our website.

Vulnerability details

Brief	Vulnerability ID	Vulnerability Category	Vulnerability Impact	Severity	CVSS 3.0 Score	Ac

Addressed a potential issue where the application could be exposed to a Null Pointer Dereference vulnerability and crash when opening certain PDFs that contain a stamp annotation missing the appearance (AP) entry, which attackers could exploit to launch a Denial of Service attack. This occurs as the application fails to validate the presence of the required appearance (AP) data before accessing stamp annotation resources and continues to dereference the associated objects without performing a prior null or validity check.	CVE-2026-3776	NULL Pointer Dereference (CWE-476)	Denial of Service	Moderate	5.5: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	•

Addressed potential issues where the application could be exposed to a Use-After-Free vulnerability and crash when handling certain documents that contain JavaScript, which attackers could exploit to execute arbitrary code. This occurs due to the use of objects that have been deleted, destroyed, or re-created without proper validation.	CVE-2026-3777	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Moderate	5.5: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H	•
	CVE-2026-3779	Use After Free (CWE-416)	Potential Arbitrary Code Execution	Important	7.8: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	•

Addressed a potential issue where the application could be exposed to an Uncontrolled Recursion vulnerability and crash when handling certain PDFs with cyclic references between objects, which attackers could exploit to cause a stack overflow. This occurs as the application fails to detect or guard against cyclic references when passing the current document as a request object into APIs.	CVE-2026-3778	Uncontrolled Recursion (CWE-674)	Stack Overflow	Moderate	6.2: AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	•

For more information, please contact the Foxit Security Response Team at security-ml@foxit.com (mailto:security-ml@foxit.com).

Foxit eSign security update

Release date: March 26, 2026

Summary

Foxit eSign has been updated to address a security issue in the signing invitation acceptance process. No customer action is required.

Vulnerability details

Brief	Vulnerability ID	Vulnerability Category	Vulnerability Impact	Severity	CVSS 3.0 Score	A
Addressed a potential insecure direct object reference (IDOR) vulnerability in the signing invitation acceptance process. Under certain conditions, this issue could have allowed an attacker to access or modify unauthorized resources by manipulating user-supplied object identifiers, potentially leading to forged signatures and compromising the integrity and authenticity of documents undergoing the signing process. The issue was caused by insufficient authorization validation on referenced resources during request processing.	CVE-2026-4947	Improper Access Control (CWE-284)	Horizontal Privilege Escalation	Important	7.1:AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N	

Solution

This issue has been resolved by enforcing proper authorization checks on object identifiers, ensuring that only the intended recipient is permitted to access and act on the invitation.

For more information, please contact the Foxit Security Response Team at security-ml@foxit.com (mailto:security-ml@foxit.com).

Security and stability enhancements in Foxit PDF Editor Cloud

Release date: February 3, 2026

Summary

Foxit PDF Editor Cloud has been updated with security and stability improvements—no action needed.

Vulnerability details

Brief	Vulnerability ID	Vulnerability Category	Vulnerability Impact	Severity	CVSS 3.0 Score	Ac

Address potential issues where the application could be exposed to a Cross-Site Scripting vulnerability when users access the File Attachments list or Layers panel with crafted payloads, which attackers could exploit to execute arbitrary JavaScript in the user's browser. This occurs due to insufficient input validation and improper output encoding in the layer name or attachment's file name fields, which allow untrusted input to be embedded into the HTML structure without adequate encoding or sanitization.	CVE-2026-1591	Cross-site Scripting (CWE-79)	Potential Arbitrary JavaScript Execution	Moderate	6.3: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N	•
	CVE-2026-1592	Cross-site Scripting (CWE-79)	Potential Arbitrary JavaScript Execution	Moderate	6.3: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N	•

For more information, please contact the Foxit Security Response Team at security-ml@foxit.com (mailto:security-ml@foxit.com).

Security and stability enhancements in Foxit eSign

Release date: January 15, 2026

Summary

Foxit eSign has been updated with security and stability improvements—no action needed.

Vulnerability details

Brief	Vulnerability ID	Vulnerability Category	Vulnerability Impact	Severity	CVSS 3.0 Score	A
Addressed a potential Cross-Site Scripting (XSS) vulnerability that could occur when an authenticated user visits a specially crafted link. In this scenario, improper handling of URL parameters could allow untrusted input to be embedded into JavaScript code or HTML attributes without adequate encoding or sanitization, potentially enabling the execution of arbitrary JavaScript in the user's browser.	CVE-2025-66523	Cross-site Scripting (CWE-79)	Potential Arbitrary JavaScript Execution	Moderate	6.1:AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N	•

Solution

This issue has been resolved by implementing appropriate input validation and output encoding to prevent the injection and execution of malicious scripts.

For more information, please contact the Foxit Security Response Team at security-ml@foxit.com (mailto:security-ml@foxit.com).

2025

2024

2023

2022

2021

2020

2019

2018

2017

2016

2015

2014

2013

2012

2011

2010

2009

Get Support

North America

1-866-693-6948

(/)

(https://www.linkedin.com/company/foxit-software-incorporated/) (https://www.facebook.com/Foxit)

Language EN

Subscribe to our newsletter for pro tips and exciting tech & trend news, or to our update bulletins for new release announcements, security & service updates, and status changes.

youremail@mail.com

Subscribe

- Newsletter
- Security Bulletins and Service Updates
- Both

Popular Features

Products

PDF Solutions

Online PDF

Company Resources

Contact Sales

1-866-680-3668

Support & General

North America

1-866-MYFOXIT

1-866-693-6948

Europe

+49 30 21783691