2026

Security updates available in PDF-XChange Editor/Tools 10.8.5.410

Released at: 21 Apr 2026

Summary

Released version 10.8.5.410, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.8.4.409
PDF-Tools	10.8.4.409

Vulnerability details

Brief	Acknowledgement
Updated third-party libraries used in the PDF-XChange products. • CVE-2025-15467	

Security updates available in PDF-XChange Editor/Tools 10.8.3.408

Released at: 24 Feb 2026

Summary

Released version 10.8.3.408, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.8.2.407
PDF-XChange PRO	10.8.2.407

Vulnerability details

Brief	Acknowledgement
Add protection against COM hijacking (unintended loading of a malicious DLL registered per-user by the CLSID of a legitimate COM server).	
Updated third-party libraries used in the PDF-XChange products.	

2025

Security updates available in PDF-XChange Editor/Tools 10.7.5.403

Released at: 28 Oct 2025

Summary
Released version 10.7.5.403, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.7.3.401
PDF-Tools	10.7.3.401
PDF-XChange PRO	10.7.3.401

Vulnerability details

Brief	Acknowledgement
Updated third-party libraries used in the PDF-XChange products.	
An out-of-bounds read vulnerability exists in the EMF functionality of PDF-XChange Editor 10.7.3.401. By using a specially crafted EMF file, an attacker could exploit this vulnerability to perform an out-of-bounds read, potentially leading to the disclosure of sensitive information.	• Discovered by KPC of Cisco Talos.
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts	• Lee Kwang-Hui

Security updates available in PDF-XChange 10.7.3.401

Released at: 23 Sep 2025

Summary
Released version 10.7.3.401, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.7.2.400
PDF-XChange PRO	10.7.2.400
PDF-Tools	10.7.2.400

Vulnerability details

Brief	Acknowledgement
Fixed a potential local privilege escalation vulnerability in the PDF-XChange Updater.	• Kolja Grassmann (Neodyme AG) working with Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 10.6.1.397

Released at: 22 Jul 2025

Summary

Released version 10.6.1.397, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.6.0.396; 10.5.2.395
PDF-Tools	10.6.0.396; 10.5.2.395
PDF-XChange PRO	10.6.0.396; 10.5.2.395

Vulnerability details

Brief	Acknowledgement
An out-of-bounds read vulnerability exists in the EMF functionality of PDF-XChange Editor version 10.5.2.395. By using a specially crafted EMF file, an attacker could exploit this vulnerability to perform an out-of-bounds read, potentially leading to the disclosure of sensitive information. • CVE-2025-27931 • CVE-2025-47152	• Discovered by KPC of Cisco Talos.
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• Suyue Guo and Tianle Yu from UCSB Seclab

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain JavaScripts	

Security updates available in PDF-XChange Editor/Tools 10.6.0.396

Released at: 06 May 2025

Summary

Released version 10.6.0.396, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.5.2.395
PDF-Tools	10.5.2.395
PDF-XChange PRO	10.5.2.395

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain U3D files and U3D streams in PDF files. • CVE-2025-6640 • CVE-2025-6641 • CVE-2025-6642 • CVE-2025-6643 • CVE-2025-6644 • CVE-2025-6645 • CVE-2025-6646 • CVE-2025-6647 • CVE-2025-6648 • CVE-2025-6649 • CVE-2025-6650	• Anonymous working with Trend Micro Zero Day Initiative • Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• Anonymous working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain PRC files and PRC streams in PDF files. • CVE-2025-6652 • CVE-2025-6653 • CVE-2025-6654 • CVE-2025-6655 • CVE-2025-6656 • CVE-2025-6657 • CVE-2025-6658 • CVE-2025-6659 • CVE-2025-6662	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain GIF files. • CVE-2025-6660	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts • CVE-2025-6661	• Suyue Guo from UCSB Seclab working with Trend Micro Zero Day Initiative • RUCSESEC
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG2000 files or JPEG2000 streams in PDF files. • CVE-2025-6651	• Anonymous working with Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 10.5.2.395

Released at: 12 Feb 2025

Summary
Released version 10.5.2.395, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.5.1.394
PDF-Tools	10.5.1.394
PDF-XChange PRO	10.5.1.394

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain RTF files.	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative

- CVE-2025-2231

Security updates available in PDF-XChange Editor/Tools 10.5.0.393

Released at: 14 Jan 2025

Summary
Released version 10.5.0.393, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.4.4.392
PDF-XChange PRO	10.4.4.392
PDF-Tools	10.4.4.392

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain XPS files.	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2025-0909 Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain U3D files and U3D streams in PDF files. • CVE-2025-0910 • CVE-2025-0911	Anonymous working with Trend Micro Zero Day Initiative
Addressed potential issues with XFA files, including untrusted URL invocation, ignoring encryption element in submit action, and importing XML data without user confirmation.	Jörn Henkel

2024

Security updates available in PDF-XChange Editor/Tools 10.4.2.392

Released at: 12 Nov 2024

Summary
Released version 10.4.4.392, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.4.3.391
PDF-XChange PRO	10.4.3.391
PDF-Tools	10.4.3.391

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• Anonymous working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain U3D files and U3D streams in PDF files.	

Security updates available in PDF-XChange Editor/Tools 10.4.2.390

Released at: 07 Oct 2024

Summary

Released version 10.4.2.390, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.4.0.388
PDF-XChange PRO	10.4.0.388
PDF-Tools	10.4.0.388

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files.	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain XPS files.	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain RTF files.	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JBIG2 files or JBIG2 streams in PDF files.	• Mat Powell of Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 10.4.1.389

Released at: 23 Sep 2024

Summary
Released version 10.4.1.389, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.4.0.388
PDF-XChange PRO	10.4.0.388

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts.	• Mat Powell of Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 10.4.0.388

Released at: 09 Sep 2024

Summary
Released version 10.4.0.388, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.3.1.387
PDF-Tools	10.3.1.387

Product	Version
PDF-XChange PRO	10.3.1.387

Vulnerability details

Brief	Acknowledgement
Updated third-party libraries used in the PDF-XChange products.	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2024-8844 • CVE-2024-8845 • CVE-2024-8849	• Mat Powell of Trend Micro Zero Day Initiative • Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JBIG2 files or JBIG2 streams in PDF files. • CVE-2024-8843	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain RTF files. • CVE-2024-8842	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain TIFF files.	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2024-8846	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts.	• Mat Powell of Trend Micro Zero Day Initiative
• CVE-2024-8847 • CVE-2024-8848	

Security updates available in PDF-XChange Editor/Tools 10.3.1.387

Released at: 18 Jun 2024

Summary
Released version 10.3.1.387, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.3.0.386
PDF-Tools	10.3.0.386
PDF-XChange PRO	10.3.0.386

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain U3D files and U3D streams in PDF files.	• Mat Powell of Trend Micro Zero Day Initiative
• CVE-2024-8812 • CVE-2024-8813 • CVE-2024-8814 • CVE-2024-8815 • CVE-2024-8816 • CVE-2024-8817 • CVE-2024-8818	

Brief	Acknowledgement
• CVE-2024-8819 • CVE-2024-8820 • CVE-2024-8821 • CVE-2024-8822	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2024-8825 • CVE-2024-8841	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain TIFF files. • CVE-2024-8834 • CVE-2024-8836	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain XPS/OXPS files. • CVE-2024-8826 • CVE-2024-8830 • CVE-2024-8831 • CVE-2024-8833 • CVE-2024-8837 • CVE-2024-8838	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative • Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2024-8828 • CVE-2024-8829 • CVE-2024-8832	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JBIG2 files or JBIG2 streams in PDF files. • CVE-2024-8823 • CVE-2024-8824 • CVE-2024-8835 • CVE-2024-8839 • CVE-2024-8840	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PNM files. • CVE-2024-8827	• Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Updated third-party libraries used in the PDF-XChange products.	

Security updates available in PDF-XChange Editor/Tools 10.3.0.386

Released at: 29 Apr 2024

Summary
Released version 10.3.0.386, which addresses potential security and stability issues. Third-party libraries are updated to the latest stable versions.

Affected versions

Product	Version
PDF-XChange Editor	10.2.1.385
PDF-XChange PRO	10.2.1.385
PDF-Tools	10.2.1.385

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files.	• Anonymous working with Trend Micro Zero Day Initiative
Updated third-party libraries used in the PDF-XChange products.	

2023

Security updates available in PDF-XChange Editor/Tools 10.1.3.383

Released at: 14 Nov 2023

Summary
Released version 10.1.3.383, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.1.2.382
PDF-Tools	10.1.2.382
PDF-XChange PRO	10.1.2.382

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• Francis Provencher {PRL} working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain TIFF files. • CVE-2024-27324	

Security updates available in PDF-XChange Editor/Tools 10.1.2.382

Released at: 23 Oct 2023

Summary
Released version 10.1.2.382, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.1.1.381
PDF-Tools	10.1.1.381
PDF-XChange PRO	10.1.1.381

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2024-27325 • CVE-2024-27328 • CVE-2024-27330 • CVE-2024-27331	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG files and JPEG streams in PDF files.	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2024-27332	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain XPS files. • CVE-2024-27326 • CVE-2024-27329	• Mat Powell of Trend Micro Zero Day Initiative
Updated third-party libraries used in the PDF-XChange products. • CVE-2023-4863	•
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2024-27327	•
Added server certificate verification into the PDF-XChange Updater to avoid downloading installers from the wrong servers. • CVE-2024-27323	• Bobby Gould and Anthony Fuller of Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 10.1.1.381

Released at: 19 Sep 2023

Summary

Released version 10.1.1.381, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.1.0.380
PDF-Tools	10.1.0.380
PDF-XChange PRO	10.1.0.380

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2023-42106 • CVE-2023-42107 • CVE-2023-42108 • CVE-2023-42109 • CVE-2023-42110 • CVE-2023-42111 • CVE-2023-42112	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPG files or JPG streams in PDF files. • CVE-2023-42111	• Mat Powell of Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 10.1.0.380

Released at: 05 Sep 2023

Summary

Released version 10.1.0.380, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	10.0.1.371
PDF-Tools	10.0.1.371
PDF-XChange PRO	10.0.1.371

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2023-42077 • CVE-2023-42080 • CVE-2023-42081 • CVE-2023-42084 • CVE-2023-42085 • CVE-2023-42086 • CVE-2023-42087	• Anonymous working with Trend Micro Zero Day Initiative • Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG files and JPEG streams in PDF files. • CVE-2023-42082 • CVE-2023-42083 • CVE-2023-42088	• Anonymous working with Trend Micro Zero Day Initiative • Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain TIFF files. • CVE-2023-42075	• Anonymous working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• Mat Powell of Trend Micro Zero Day Initiative • rgod working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2023-42071 • CVE-2023-42076	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG2000 files and JPEG2000 streams in PDF files. • CVE-2022-37351 • CVE-2023-39483 • CVE-2023-39484 • CVE-2023-39485 • CVE-2023-39486 • CVE-2023-42045 • CVE-2023-42046 • CVE-2023-42047 • CVE-2023-42048 • CVE-2023-42072 • CVE-2023-42078 • CVE-2023-42079	• Mat Powell of Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 10.0.0.370

Released at: 14 Jun 2023

Summary

Released version 10.0.0.370, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	9.5.368.0
PDF-Tools	9.5.368.0
PDF-XChange PRO	9.5.368.0

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts. • CVE-2023-40471 • CVE-2023-40472 • CVE-2023-42040 • CVE-2023-42041 • CVE-2023-42042 • CVE-2023-42043 • CVE-2023-42044 • CVE-2023-42070 • CVE-2023-42073 • CVE-2023-42074	• kimiya working with Trend Micro Zero Day Initiative • Mat Powell of Trend Micro Zero Day Initiative • Rocco Calvi (@TecR0c) with TecSecurity working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2023-42049 • CVE-2023-42050	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PRC files and PRC streams in PDF files. • CVE-2023-42051 • CVE-2023-42052 • CVE-2023-42053 • CVE-2023-42054 • CVE-2023-42055	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2023-42056 • CVE-2023-42059 • CVE-2023-42060 • CVE-2023-42061 • CVE-2023-42063	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain U3D files and U3D streams in PDF files. • CVE-2023-42057 • CVE-2023-42058 • CVE-2023-42062 • CVE-2023-42064	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JBIG2 files or JBIG2 streams in PDF files. • CVE-2023-42067 • CVE-2023-42068	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2023-42069	• Anonymous working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain JPEG2000 files or JPEG2000 streams in PDF files. • CVE-2023-42065 • CVE-2023-42066	

Security updates available in PDF-XChange Editor/Tools 9.5.368.0

Released at: 05 Apr 2023

Summary
Released version 9.5.368.0, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	9.5.367.0
PDF-Tools	9.5.367.0
PDF-XChange PRO	9.5.367.0

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain XPS/OXPS files. • CVE-2023-40469	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts.	• kimiya working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2023-39506	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2023-40468	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG2000 files or JPEG2000 streams in PDF files. • CVE-2023-40470	• Mat Powell of Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 9.5.367.0

Released at: 06 Mar 2023

Summary

Released version 9.5.367.0, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	9.5.366.0
PDF-Tools	9.5.366.0
PDF-XChange PRO	9.5.366.0

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• hades_kito working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain JPEG files or JPEG streams in PDF files. • CVE-2023-39497 • CVE-2023-39498 • CVE-2023-39499 • CVE-2023-39500	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain XPS/OXPS files. • CVE-2023-39494 • CVE-2023-39501 • CVE-2023-39502 • CVE-2023-39503 • CVE-2023-39504	• Andrea Micalizzi aka rgod working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain TIFF files. • CVE-2023-39491 • CVE-2023-39496	• hades_kito working with Trend Micro Zero Day Initiative • Andrea Micalizzi aka rgod working with Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts. • CVE-2023-39493	• Andrea Micalizzi aka rgod working with Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2023-39495 • CVE-2023-39505	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2023-39490 • CVE-2023-39492 •	• hades_kito working with Trend Micro Zero Day Initiative

2022

Security updates available in PDF-XChange Editor/Tools 9.5.366.0

Released at: 12 Dec 2022

Summary
Released version 9.5.366.0, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	9.5.365.0
PDF-Tools	9.5.365.0
PDF-XChange PRO	9.5.365.0

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain TIFF files. • CVE-2023-39488	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement

- CVE-2023-39489

Security updates available in PDF-XChange Editor/Tools 9.5.365.0

Released at: 28 Nov 2022

Summary
Released version 9.5.365.0, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	9.4.364.0
PDF-Tools	9.4.364.0
PDF-XChange PRO	9.4.364.0

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2023-27342 • CVE-2023-27343	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG2000 files or JPEG2000 streams in PDF files. • CVE-2023-39485 • CVE-2023-39486	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain U3D files or U3D streams in PDF files. • CVE-2022-42394	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain TIFF files. • CVE-2023-27348	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2023-27344 • CVE-2023-27345	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts. • CVE-2023-39487	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PNG files. • CVE-2023-27339	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement

- CVE-2023-27340

Security updates available in PDF-XChange Editor/Tools 9.4.364.0

Released at: 27 Sep 2022

Summary

Release version 9.4.364.0, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	9.4.362.0
PDF-Tools	9.4.362.0
PDF-XChange PRO	9.4.362.0

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain U3D files or U3D streams in PDF files.	• Mat Powell of Trend Micro Zero Day Initiative • Tran Van Khang (VinCSS) • Rocco Calvi (@TerR0C) • Anonymous working with Trend Micro Zero Day Initiative

- CVE-2022-41143
- CVE-2022-41144
- CVE-2022-41145
- CVE-2022-41146
- CVE-2022-41147
- CVE-2022-41148
- CVE-2022-41149
- CVE-2022-41150
- CVE-2022-41151
- CVE-2022-41152
- CVE-2022-41153
- CVE-2022-42369

- CVE-2022-42370
- CVE-2022-42371
- CVE-2022-42372
- CVE-2022-42373
- CVE-2022-42374

Brief	Acknowledgement
• CVE-2022-42375 • CVE-2022-42376 • CVE-2022-42377 • CVE-2022-42378 • CVE-2022-42379 • CVE-2022-42380 • CVE-2022-42381 • CVE-2022-42382 • CVE-2022-42383 • CVE-2022-42384 • CVE-2022-42385 • CVE-2022-42386 • CVE-2022-42387 • CVE-2022-42388 • CVE-2022-42389 • CVE-2022-42390 • CVE-2022-42391 • CVE-2022-42392 • CVE-2022-42393	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain TIFF files. • CVE-2023-42416 • CVE-2023-42417 • CVE-2023-42418 • CVE-2023-42419 • CVE-2023-42420 • CVE-2023-42421 • CVE-2023-42423 • CVE-2023-27338 • CVE-2023-27341	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
reference to the object that has been deleted without proper validation when handling certain EMF files. • CVE-2022-42404 • CVE-2022-42405 • CVE-2022-42406 • CVE-2022-42407 • CVE-2022-42408	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JBIG2 files or JBIG2 streams in PDF files. • CVE-2022-42398 • CVE-2022-42409	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG2000 files or JPEG2000 streams in PDF files. • CVE-2022-42411 • CVE-2022-42412 • CVE-2022-42413 • CVE-2022-42414 • CVE-2022-42415	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PDF files. • CVE-2022-42399	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2022-42400 • CVE-2022-42401 • CVE-2022-42402 • CVE-2022-42403	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PGM files. • CVE-2022-42410	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts. • CVE-2023-27337	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain XPS/OXPS files. • CVE-2022-42395 • CVE-2022-42396 • CVE-2022-42397	• Tran Van Khang - khangkito (VinCSS) working with Trend Micro Zero Day Initiative

Security updates available in PDF-XChange Editor/Tools 9.4.362.0

Released at: 08 Aug 2022

Summary
Release version 9.4.362.0, which addresses potential security and stability issues.

Affected versions

Product	Version
PDF-XChange Editor	9.3.361.0
PDF-Tools	9.3.361.0
PDF-XChange PRO	9.3.361.0

Vulnerability details

Brief	Acknowledgement
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JavaScripts • CVE-2022-37349 • CVE-2022-37350 • CVE-2022-37365 • CVE-2022-37367 • CVE-2022-37366 • CVE-2022-37368	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain EMF/WMF files. • CVE-2022-37364 • CVE-2022-37360 • CVE-2022-37353 • CVE-2022-37352 • CVE-2022-37363	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JBIG2 files or JBIG2 streams in PDF files.	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2022-37369 • CVE-2022-37370 • CVE-2022-37371 • CVE-2022-37372 • CVE-2022-37373	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PBM/PGM/PPM files. • CVE-2022-37356 • CVE-2022-37362	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG files or JPEG streams in PDF files. • CVE-2022-37354 • CVE-2022-37355 • CVE-2022-37358 • CVE-2022-37359	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain JPEG2000 files or JPEG2000 streams in PDF files. • CVE-2022-37361 • CVE-2023-32158 • CVE-2023-32159	• Mat Powell of Trend Micro Zero Day Initiative

Brief	Acknowledgement
• CVE-2023-32160 • CVE-2022-37375	
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain ICO files. • CVE-2022-37357	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PNG files. • CVE-2022-37374	• Mat Powell of Trend Micro Zero Day Initiative
Addressed potential issues where the application could be exposed to Use-after-Free, Out-of-Bounds Read, or Type Confusion vulnerability and crash, which could be exploited by attackers to execute remote code or disclose information. This occurs due to the access of null pointer/wild pointer or reference to the object that has been deleted without proper validation when handling certain PNG files. • CVE-2023-32161	• Mat Powell of Trend Micro Zero Day Initiative