

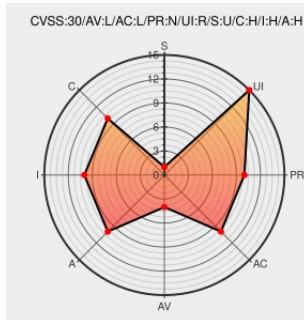


# CVE-2020-10893

Published on: 04/22/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:34 PM UTC

## CVE-2020-10893

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Phantompdf](#) from [Foxitsoftware](#) contain the following vulnerability:

This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. 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 handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10189.

CVE-2020-10893 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Foxit - PhantomPDF** version **9.7.1.29511**

CVSS3 Score: **7.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>LOCAL</b>     | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                         | Tags                                                                                                                                        | Link                                                                                                                                                                                                                  |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Bulletins   Foxit Software | <a href="#">Vendor Advisory</a><br><a href="#">www.foxitsoftware.com</a><br><a href="#">text/html</a>                                       |  MISC <a href="http://www.foxitsoftware.com/support/security-bulletins.php">www.foxitsoftware.com/support/security-bulletins.php</a> |
| ZDI-20-521   Zero Day Initiative    | <a href="#">Third Party Advisory</a><br><a href="#">VDB Entry</a><br><a href="#">www.zerodayinitiative.com</a><br><a href="#">text/html</a> |  MISC <a href="http://www.zerodayinitiative.com/advisories/ZDI-20-521/">www.zerodayinitiative.com/advisories/ZDI-20-521/</a>         |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type                                                             | Vendor                        | Product                    | Version | Update | Edition | Language |
|------------------------------------------------------------------|-------------------------------|----------------------------|---------|--------|---------|----------|
| Application                                                      | <a href="#">Foxitsoftware</a> | <a href="#">Phantompdf</a> | All     | All    | All     | All      |
| Application                                                      | <a href="#">Foxitsoftware</a> | <a href="#">Reader</a>     | All     | All    | All     | All      |
| Operating System                                                 | <a href="#">Microsoft</a>     | <a href="#">Windows</a>    | -       | All    | All     | All      |
| Operating System                                                 | <a href="#">Microsoft</a>     | <a href="#">Windows</a>    | -       | All    | All     | All      |
| <a href="#">cpe:2.3:a:foxitsoftware:phantompdf:*.***.***.***</a> |                               |                            |         |        |         |          |
| <a href="#">cpe:2.3:a:foxitsoftware:reader:*.***.***.***</a>     |                               |                            |         |        |         |          |
| <a href="#">cpe:2.3:o:microsoft:windows:-.***.***.***</a>        |                               |                            |         |        |         |          |
| <a href="#">cpe:2.3:o:microsoft:windows:-.***.***.***</a>        |                               |                            |         |        |         |          |

## Discovery Credit

Mat Powell of Trend Micro Zero Day Initiative

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

