

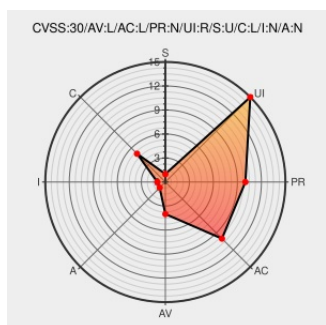


# CVE-2020-17429

Published on: 02/09/2021 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:30 PM UTC

## CVE-2020-17429

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

Certain versions of [Foxit Studio Photo](#) from [Foxitsoftware](#) contain the following vulnerability:

This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit Studio Photo 3.6.6.922. 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 CMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-11337.

CVE-2020-17429 has been assigned by zdi-disclosures@trendmicro.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Foxit - Studio Photo** version **3.6.6.922**

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.3 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| NETWORK                | MEDIUM            | NONE                |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| PARTIAL                | NONE              | NONE                |

CVE References

| Description                         | Tags                                                                                                           | Link                                                                                                                                                                                                                    |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Bulletins   Foxit Software | <div>Not Applicable</div> <div>www.foxitsoftware.com</div> <div>text/html</div>                                |  MISC <a href="http://www.foxitsoftware.com/support/security-bulletins.html">www.foxitsoftware.com/support/security-bulletins.html</a> |
| ZDI-20-1340   Zero Day Initiative   | <div>Third Party Advisory</div> <div>VDB Entry</div> <div>www.zerodayinitiative.com</div> <div>text/html</div> |  MISC <a href="http://www.zerodayinitiative.com/advisories/ZDI-20-1340/">www.zerodayinitiative.com/advisories/ZDI-20-1340/</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="#">Foxit Studio Photo</a> | 3.6.6.922 | All    | All     | All      |
| Application | <a href="#">Foxitsoftware</a> | <a href="#">Foxit Studio Photo</a> | 3.6.6.922 | All    | All     | All      |

cpe:2.3:a:foxitsoftware:foxit\_studio\_photo:3.6.6.922:\*:\*:\*:\*:\*:

cpe:2.3:a:foxitsoftware:foxit\_studio\_photo:3.6.6.922:\*:\*:\*:\*:\*:

Discovery Credit

Mat Powell of Trend Micro Zero Day Initiative

← Previous ID

Next ID →