



CVE-2021-30354

Published on: 09/01/2021 12:00:00 AM UTC

Last Modified on: 09/10/2021 02:55:00 PM UTC

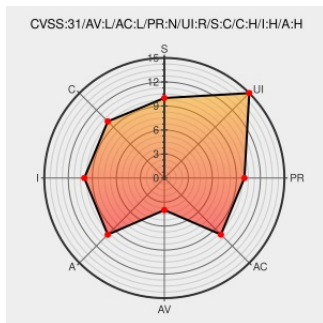
CVE-2021-30354

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Kindle](#) from [Amazon](#) contain the following vulnerability:

Amazon Kindle e-reader prior to and including version 5.13.4 contains an Integer Overflow that leads to a Heap-Based Buffer Overflow in function CBig2Image::expand() and results in a memory corruption that leads to code execution when parsing a crafted PDF book.

CVE-2021-30354 has been assigned by cve@checkpoint.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.6 - HIGH**

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

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Do you like to read? I can take over your Kindle with an e-book - Check Point Research	research.checkpoint.com text/html	MISC research.checkpoint.com/2021/i-can-take-over-your-kindle/

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Amazon	Kindle	-	All	All	All
Operating System	Amazon	Kindle Firmware	All	All	All	All
cpe:2.3:h:amazon:kindle:-:*****:						
cpe:2.3:o:amazon:kindle_firmware:*****:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @_CPRresearch_	[CPR-Zero] CVE-2021-30354 (Kindle): Integer Overflow leading to Heap-based Buffer Overflow in... twitter.com/i/web/status/1...	2021-08-19 12:51:08
 @CVEreport	CVE-2021-30354 : Amazon Kindle e-reader prior to and including version 5.13.4 contains an Integer Overflow that lea... twitter.com/i/web/status/1...	2021-09-01 18:05:51
 @EWS_Bot	Potentially Critical CVE Detected! CVE-2021-30354 Description: CVE-2021-30354 Amazon Kindle e-reader prior to and i... twitter.com/i/web/status/1...	2021-09-01 19:00:05

[← 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)