

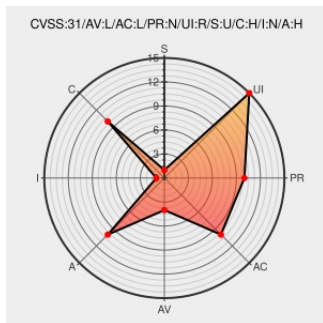


CVE-2021-3548

Published on: 05/26/2021 12:00:00 AM UTC

Last Modified on: 02/12/2023 11:12:07 PM UTC

CVE-2021-3548

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

Certain versions of [Dmg2img](#) from [Dmg2img Project](#) contain the following vulnerability:

A flaw was found in dmg2img through 20170502. dmg2img did not validate the size of the read buffer during memcpy() inside the main() function. This possibly leads to memory layout information leaking in the data. This might be used in a chain of vulnerability in order to reach code execution.

CVE-2021-3548 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.1 - HIGH**

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

CVSS2 Score: **5.8 - MEDIUM**

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

CVE References

Description	Tags	Link
1959585 – (CVE-2021-3548) CVE-2021-3548 dmg2img: OOB in dmg2img.c memcpy() causing undefined behavior	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=1959585

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
Application	Dmg2img Project	Dmg2img	All	All	All	All
cpe:2.3:a:dmg2img_project:dmg2img:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-3548 : A flaw was found in dmg2img through 20170502. dmg2img did not validate the size of the read buffer... twitter.com/i/web/status/1...	2021-05-26 21:06:22
 /r/netcve	CVE-2021-3548	2021-05-26 21:41:41

[← 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](#)