



CVE-2020-6076

Published on: 05/06/2020 12:00:00 AM UTC

Last Modified on: 07/28/2022 05:12:00 PM UTC

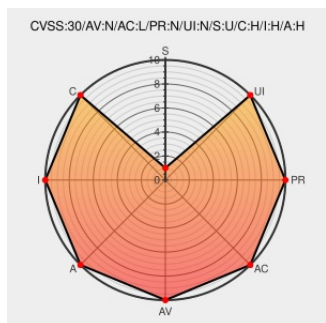
CVE-2020-6076

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Imagegear](#) from [Accusoft](#) contain the following vulnerability:

An exploitable out-of-bounds write vulnerability exists in the igcore19d.dll ICO icoread parser of the Accusoft ImageGear 19.5.0 library. A specially crafted ICO file can cause an out-of-bounds write, resulting in a remote code execution. An attacker needs to provide a malformed file to the victim to trigger the vulnerability.

CVE-2020-6076 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector

Attack Complexity

Privileges Required

User Interaction

NETWORK

LOW

NONE

REQUIRED

Scope

Confidentiality Impact

Integrity Impact

Availability Impact

UNCHANGED

HIGH

HIGH

HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

TALOS-2020-0999 || Cisco Talos Intelligence Group - Comprehensive Threat Intelligence

[Third Party Advisory](#)
[talosintelligence.com](#)
[text/html](#)

[MISC](#)
[talosintelligence.com/vulnerability_reports/TALOS-2020-0999](#)

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	Accusoft	Imagegear	19.5.0	All	All	All
Application	Accusoft	Imagegear	19.5.0	All	All	All
cpe:2.3:a:accusoft:imagegear:19.5.0:*:*:*:*:*:						
cpe:2.3:a:accusoft:imagegear:19.5.0:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? An exploitable out-of-bounds write vulne... CVE-2020-6076 Link for more: alerts.remotelyrmm.com/CVE-2020-6076	2022-04-19 19:35:19

[← Previous ID](#)

[Next ID →](#)