



CVE-2021-21824

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2021-21824
State	PUBLIC
Assigner	talos-cna@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-06-11 17:15:00 UTC
Updated	2022-08-24 21:57:00 UTC
Description	An out-of-bounds write vulnerability exists in the JPG Handle_JPEG420 functionality of Accusoft ImageGear 19.9. A special

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Accusoft	Imagegear	19.9	All	All	All

References

Reference	Source	Link	Tags
TALOS-2021-1289 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	MISC	talosintelligence.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375619](#) Accusoft ImageGear Multiple Vulnerabilities (TALOS-2021-1257,TALOS-2021-1261,TALOS-2021-1289,TALOS-2021-1264,TALOS-2021-1276,TALOS-2021-1286,TALOS-2021-1275,TALOS-2021-1296)

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report