



CVE-2021-29098

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

Summary

CVE	CVE-2021-29098
State	PUBLIC
Assigner	psirt@esri.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-03-25 21:15:00 UTC
Updated	2023-11-07 03:32:00 UTC
Description	Multiple uninitialized pointer vulnerabilities when parsing a specially crafted file in Esri ArcReader, ArcGIS Desktop, ArcGIS

Risk And Classification

Problem Types: CWE-824

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Esri	Arcgis	All	All	All	All
Application	Esri	Arcgis Desktop	All	All	All	All
Application	Esri	Arcgis Pro	All	All	All	All
Application	Esri	Arcreader	All	All	All	All

References

Reference	Source	Link	Tags
ArcGIS general raster security update	CONFIRM	www.esri.com	
ZDI-21-362 Zero Day Initiative	MISC	www.zerodayinitiative.com	
ZDI-21-361 Zero Day Initiative	MISC	www.zerodayinitiative.com	
ZDI-21-372 Zero Day Initiative	MISC	www.zerodayinitiative.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

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