

CVE-2021-22204

Perl ExifTool Remote Code Execution Vulnerability

CISA KEV since Nov 17, 2021

Actively exploited

Public exploit module (Metasploit)

Improper neutralization of user data in the DjVu file format in ExifTool versions 7.44 and up allows arbitrary code execution when parsing the malicious image

EVRS 84 /100 Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.999 99.98th percentile · FIRST	CISA DEADLINE Dec 1, 2021 KEV since 2021 · listed over a year
---	--	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
exiftool	≥ 7.44 < 12.24	no fixed version listed	NVD
debian linux	9.0 10.0	no fixed version listed	NVD
fedora	32 33 34	no fixed version listed	NVD

Sources

Vendor guidance	github.com/exiftool/exiftool/commit/cf0f4e7dcd024ca99615bfd1102a841a25dde031#diff-fa0d652d10dbcd246e6b1df16c1e992931d3bb717a7e36157596b76bdadb3800	Additional guidance	debian.org/security/2021/dsa-4910
NVD	nvd.nist.gov/vuln/detail/CVE-2021-22204	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-9350	Current data	evulnable.com/vulnerability-management/cve/CVE-2021-22204

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.