# CVE Detail – CVE-2021-22204

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

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.9978

## CVSS Scoring

CVSS v3.1 Score: 6.8

Severity: MEDIUM

## CISA KEV

KEV is present

## Mapped CWE(s)

* CWE-94: Improper Control of Generation of Code ('Code Injection')

## CAPEC(s)

* CAPEC-242: Code Injection
* CAPEC-35: Leverage Executable Code in Non-Executable Files
* CAPEC-77: Manipulating User-Controlled Variables

## ATT&CK Techniques

* T1027.009: Embedded Payloads
* T1564.009: Resource Forking
* T1027.006: HTML Smuggling

## Used By (Actors/Tools)

* Pikabot (malware)
* macOS.OSAMiner (malware)
* EnvyScout (malware)
* Emotet (malware)
* DUSTTRAP (malware)
* BADHATCH (malware)
* DUSTPAN (malware)
* Moneybird (malware)
* Keydnap (malware)
* IcedID (malware)
* CHIMNEYSWEEP (malware)
* MultiLayer Wiper (malware)
* Netwalker (malware)
* SMOKEDHAM (malware)
* Uroburos (malware)
* DEADEYE (malware)
* ComRAT (malware)
* QakBot (malware)
* OSX/Shlayer (malware)
* DEADWOOD (malware)
* Dtrack (malware)
* Invoke-PSImage (tool)
* Lazarus Group (intrusion-set)
* TA577 (intrusion-set)
* APT29 (intrusion-set)
* C0021 (campaign)
* Moonstone Sleet (intrusion-set)

## Affected Products

* cpe:2.3:a:exiftool\_project:exiftool:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:32:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:33:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:34:\*:\*:\*:\*:\*:\*:\*