# CVE Detail – CVE-2021-32617

Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An inefficient algorithm (quadratic complexity) was found in Exiv2 versions v0.27.3 and earlier. The inefficient algorithm is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.4. Note that this bug is only triggered when \_writing\_ the metadata, which is a less frequently used Exiv2 operation than \_reading\_ the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `rm`.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.234

## CVSS Scoring

CVSS v3.1 Score: 4.7

Severity: MEDIUM

## Mapped CWE(s)

* CWE-400: Uncontrolled Resource Consumption

## CAPEC(s)

* CAPEC-147: XML Ping of the Death
* CAPEC-227: Sustained Client Engagement
* CAPEC-492: Regular Expression Exponential Blowup

## ATT&CK Techniques

* T1499: Endpoint Denial of Service

## Used By (Actors/Tools)

* OnionDuke (malware)
* ZxShell (malware)
* Sandworm Team (intrusion-set)

## Affected Products

* cpe:2.3:a:exiv2:exiv2:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:33:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:34:\*:\*:\*:\*:\*:\*:\*