

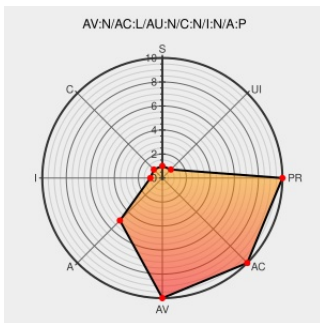


CVE-2005-4676

Published on: 12/31/2005 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:21 PM UTC

CVE-2005-4676

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Exiv2](#) from [Andreas Huggel](#) contain the following vulnerability:

Buffer overflow in Andreas Huggel Exiv2 before 0.9 does not null terminate strings before calling the sscanf function, which allows remote attackers to cause a denial of service (application crash) via images with crafted IPTC metadata.

CVE-2005-4676 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Exiv2 - Exif and Iptc metadata manipulation library and tools

[home.arcor.de](#)
[text/html](#)

[CONFIRM](#) [home.arcor.de/ahuggel/exiv2/changelog.html](#)

Exiv2 Corrupted EXIF Data Denial Of Service Vulnerability

[Exploit](#)
[Patch](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 16400](#)

0000447: Buffer overflow in sscanf - Issue Tracker

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[MISC](#)
[dev.robotbattle.com/mantis/bug_view_advanced_page.php?bug_id=447](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF](#) [exiv2-iptc-metadata-dos\(24349\)](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN](#) [ADV-2006-0345](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Andreas Huggel	Exiv2	0.3	All	All	All
Application	Andreas Huggel	Exiv2	0.4	All	All	All
Application	Andreas Huggel	Exiv2	0.5	All	All	All
Application	Andreas Huggel	Exiv2	0.6	All	All	All
Application	Andreas Huggel	Exiv2	0.6.1	All	All	All
Application	Andreas Huggel	Exiv2	0.6.2	All	All	All
Application	Andreas Huggel	Exiv2	0.7	All	All	All
Application	Andreas Huggel	Exiv2	0.8	All	All	All
Application	Andreas Huggel	Exiv2	0.3	All	All	All
Application	Andreas Huggel	Exiv2	0.4	All	All	All
Application	Andreas Huggel	Exiv2	0.5	All	All	All
Application	Andreas Huggel	Exiv2	0.6	All	All	All
Application	Andreas Huggel	Exiv2	0.6.1	All	All	All
Application	Andreas Huggel	Exiv2	0.6.2	All	All	All
Application	Andreas Huggel	Exiv2	0.7	All	All	All
Application	Andreas Huggel	Exiv2	0.8	All	All	All

```
cpe:2.3:a:andreas_huggel:exiv2:0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:andreas_huggel:exiv2:0.4:*:*:*:*:*:
```

```
cpe:2.3:a:andreas_huggel:exiv2:0.5:*:*:*:*:*:
```

```
cpe:2.3:a:andreas_huggel:exiv2:0.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:andreas_huggel:exiv2:0.6.1:*.~*~*~*~*~*~*
```

```
cpe:2.3:a:andreas_huggel:exiv2:0.6.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:andreas_huggel:exiv2:0.7:*:*:*:*:*:
```

cpe:2.3:a:andreas_huggel:exiv2:0.8:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.3:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.4:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.5:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.6:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.6.1:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.6.2:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.7:*****:
cpe:2.3:a:andreas_huggel:exiv2:0.8:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023  |

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](#).

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