

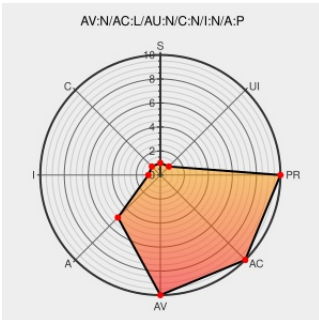


CVE-2005-1275

Published on: 04/25/2005 04:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:25 AM UTC

CVE-2005-1275

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

Certain versions of [Graphicsmagick](#) from [Graphicsmagick](#) contain the following vulnerability:

Heap-based buffer overflow in the ReadPNMImage function in pnm.c for ImageMagick 6.2.1 and earlier allows remote attackers to cause a denial of service (application crash) via a PNM file with a small colors value.

CVE-2005-1275 has been assigned by secalert@redhat.com 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

Advisories - Mandriva

www.mandriva.com
text/html

[MANDRAKE MDKSA-2005:107](#)

Repository / Oval Repository

oval.cisecurity.org
text/html

[OVAL oval:org.mitre.oval:def:10003](#)

Bugtraq: [Overflow.pl] ImageMagick
ReadPNMImage() Heap Overflow

[Exploit](#)
[seclists.org](#)
text/html

[BUGTRAQ 20050424 \[Overflow.pl\] ImageMagick
ReadPNMImage\(\) Heap Overflow](#)

ImageMagick: Changelog

[Patch](#)
www.imagemagick.org
text/html

[CONFIRM](#)
www.imagemagick.org/script/changelog.php

Support

www.redhat.com
text/html

[REDHAT RHSA-2005:413](#)

Gentoo Bug 90423 - media-gfx/imagemagick-6.* - XWD Infinite loop DoS	Exploit bugs.gentoo.org text/html	MISC bugs.gentoo.org/show_bug.cgi?id=90423
ImageMagick PNM Image Decoding Remote Buffer Overflow Vulnerability	Exploit cve.report (archive) text/html	MISC BID 13351
404 Not Found	Exploit www.overflow.pl text/plain Inactive Link Not Archived	MISC www.overflow.pl/adv/imheapoverflow.txt
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:711

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	Graphicsmagick	Graphicsmagick	1.0	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.0.6	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1.3	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1.4	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1.5	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.0	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.0.6	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1.3	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1.4	All	All	All
Application	Graphicsmagick	Graphicsmagick	1.1.5	All	All	All
Application	Imagemagick	Imagemagick	6.0	All	All	All
Application	Imagemagick	Imagemagick	6.0.1	All	All	All
Application	Imagemagick	Imagemagick	6.0.2	All	All	All
Application	Imagemagick	Imagemagick	6.0.2.5	All	All	All
Application	Imagemagick	Imagemagick	6.0.3	All	All	All
Application	Imagemagick	Imagemagick	6.0.4	All	All	All
Application	Imagemagick	Imagemagick	6.0.5	All	All	All

[illegible]

Application	Imagemagick	Imagemagick	6.2.0.4	All	All	All
Application	Imagemagick	Imagemagick	6.2.0.7	All	All	All
Application	Imagemagick	Imagemagick	6.2.1	All	All	All
cpe:2.3:a:graphicsmagick:graphicsmagick:1.0:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.0.6:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1.3:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1.4:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1.5:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.0:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.0.6:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1.3:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1.4:*:*:*:*:*:						
cpe:2.3:a:graphicsmagick:graphicsmagick:1.1.5:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.1:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.2:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.2.5:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.3:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.4:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.5:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.6:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.7:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.0.8:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.1:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.1.1.6:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.1.2:*:*:*:*:*:						
cpe:2.3:a:imagemagick:imagemagick:6.1.3:*:*:*:*:*:						

```
cpe:2.3:a:imagemagick:imagemagick:6.1.4.*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.5:*:*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.6:*:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.7:::*:*:*:*.*
```

```
cpe:2.3:a:image Magick:imagemagick:6.1.8.*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.2.0.4.*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.2.0.7:*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.2.1:*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0:*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.2.5:*:*:*:*:*:*
```

```
cpe:2.3:a:image Magick:imagemagick:6.0.3.*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.4.*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.7:*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.1.6:*:*:*:*:*.*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.2:*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.3.*:*:*:*:*:*.*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.4.*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:imagemagick:6.1.5.*:*:*:*:*:*:
```

```
cpe:2.3:a:image Magick:imagemagick:6.1.6.*:*:*:*:*:*
```

```
cpe:2.3:a:imagemagick:image Magick:6.1.7:::*:*:*.*.*
```

```
cpe:2.3:a:image Magick:imagemagick:6.1.8.*:*:*:*:*:*
```

cpe:2.3:a:imagemagick:imagemagick:6.2.*:*:*:*:*:
cpe:2.3:a:imagemagick:imagemagick:6.2.0.4.*:*:*:*:*:
cpe:2.3:a:imagemagick:imagemagick:6.2.0.7.*:*:*:*:*:
cpe:2.3:a:imagemagick:imagemagick:6.2.1.*:*:*:*:*:

```
cpe:2.3:a:imagemagick:imagemagick:6.2.0.4:*.***:***:***:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.2.0.7:*:*:*:*:*:
```

```
cpe:2.3:a:imagemagick:imagemagick:6.2.1:*:*:*:*:*.*
```

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