



# CVE-2010-1519

Published on: 08/13/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:04 PM UTC

## CVE-2010-1519

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

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

Multiple integer overflows in glpng.c in glpng 1.45 allow context-dependent attackers to execute arbitrary code via a crafted PNG image, related to (1) the pngLoadRawF function and (2) the pngLoadF function, leading to heap-based buffer overflows.

CVE-2010-1519 has been assigned by PSIRT-CNA@flexerasoftware.com to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access  
Vector

**NETWORK**

Access  
Complexity

**MEDIUM**

Authentication

**NONE**

Confidentiality  
Impact

**PARTIAL**

Integrity  
Impact

**PARTIAL**

Availability  
Impact

**PARTIAL**

## CVE References

Description

Tags

Link

Support / Security / Advisories // MDVSA-2010:179 | Mandriva

[www.mandriva.com](http://www.mandriva.com/text/html)  
[text/html](#)

[MANDRIVA MDVSA-2010:179](#)

SecurityFocus

[www.securityfocus.com](http://www.securityfocus.com/text/html)  
[text/html](#)

[BUGTRAQ 20100811 Secunia Research: glpng PNG Processing Two Integer Overflow Vulnerabilities](#)

glpng PNG Processing Integer Overflow Vulnerabilities - Secunia.com

[Vendor Advisory](#)  
[web.archive.org](http://web.archive.org/text/html)  
[text/html](#)

[SECUNIA 40354](#)

Research - Community

[Vendor Advisory](#)  
[web.archive.org](http://web.archive.org/text/html)  
[text/html](#)

[MISC secunia.com/secunia\\_research/2010-87/](#)

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,

are more appropriate for your purposes. CVEreport does not necessarily endorse the views expressed, or content that are linked, presented on these sites. 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](mailto: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                           | <a href="#">Glpng</a> | <a href="#">Glpng</a> | 1.45    | All    | All     | All      |
| Application                           | <a href="#">Glpng</a> | <a href="#">Glpng</a> | 1.45    | All    | All     | All      |
| cpe:2.3:a:glpng:glpng:1.45:*:*:*:*:*: |                       |                       |         |        |         |          |
| cpe:2.3:a:glpng:glpng:1.45:*:*:*:*:*: |                       |                       |         |        |         |          |

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)