

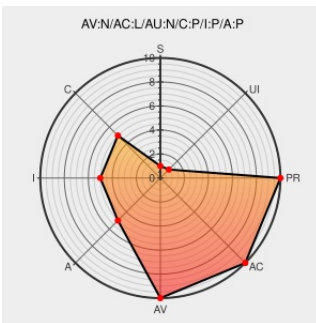


CVE-2009-4230

Published on: 12/08/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:23 PM UTC

CVE-2009-4230

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

Certain versions of [IPIImage Server](#) from [Ruven Pillay](#) contain the following vulnerability:

Multiple stack-based buffer overflows in src/Task.cc in the FastCGI program in IPIImage Server before 0.9.8 might allow remote attackers to execute arbitrary code via vectors associated with crafted arguments to the (1) RGN::run, (2) JTLS::run, or (3) SHD::run function. NOTE: some of these details are obtained from third party information.

CVE-2009-4230 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IPIImage » Blog

[Vendor Advisory](#)
[iipimage.sourceforge.net](#)
[text/html](#)

[CONFIRM](#) iipimage.sourceforge.net/blog/

IPIImage Server Buffer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com

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

[SECUNIA 37565](#)

Version 0.9.8 of IPIImage | freshmeat.net

[freshmeat.net](#)
[text/html](#)

[CONFIRM](#) freshmeat.net/projects/iipimage/releases/309013

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

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ruven Pillay	lipimage Server	0.9.3	All	All	All
Application	Ruven Pillay	lipimage Server	0.9.4	All	All	All
Application	Ruven Pillay	lipimage Server	0.9.5	All	All	All
Application	Ruven Pillay	lipimage Server	0.9.6	All	All	All
Application	Ruven Pillay	lipimage Server	All	All	All	All
Application	Ruven Pillay	lipimage Server	0.9.3	All	All	All
Application	Ruven Pillay	lipimage Server	0.9.4	All	All	All
Application	Ruven Pillay	lipimage Server	0.9.5	All	All	All
Application	Ruven Pillay	lipimage Server	0.9.6	All	All	All
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.3:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.4:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.5:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.6:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.3:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.4:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.5:*****:						
cpe:2.3:a:ruven_pillay:lipimage_server:0.9.6:*****:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

