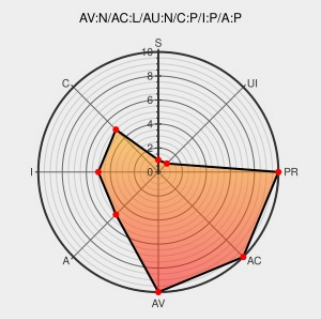
CVE-2009-4230

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 Iipimage Server from Ruven Pillay contain the following vulnerability:

Multiple stack-based buffer overflows in src/Task.cc in the FastCGI program in IIPImage 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 cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
IIPImage » Blog	Vendor Advisory, iipimage.sourceforge.net, text/html	CONFIRM iipimage.sourceforge.net/blog/
IIPImage Server Buffer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory, web.archive.org, text/html	SECUNIA 37565
Version 0.9.8 of IIPImage | freshmeat.net	freshmeat.net, text/html	CONFIRM freshmeat.net/projects/iipimage/releases/309013

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	Ruven Pillay	Iipimage Server	0.9.3	All	All	All
Application	Ruven Pillay	Iipimage Server	0.9.4	All	All	All
Application	Ruven Pillay	Iipimage Server	0.9.5	All	All	All
Application	Ruven Pillay	Iipimage Server	0.9.6	All	All	All
Application	Ruven Pillay	Iipimage Server	All	All	All	All
Application	Ruven Pillay	Iipimage Server	0.9.3	All	All	All
Application	Ruven Pillay	Iipimage Server	0.9.4	All	All	All
Application	Ruven Pillay	Iipimage Server	0.9.5	All	All	All
Application	Ruven Pillay	Iipimage Server	0.9.6	All	All	All

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.6:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:*:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.3:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.4:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.5:*:*:*:*:*:*:*:

cpe:2.3:a:ruven_pillay:iipimage_server:0.9.6:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report