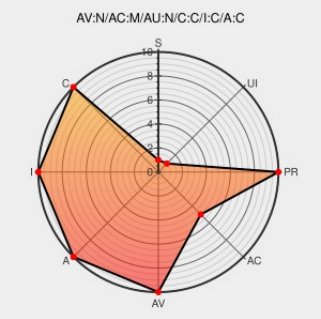
CVE-2009-4769

Published on: 04/20/2010 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:22 PM UTC

CVE-2009-4769

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Httpdx from Jasper contain the following vulnerability:

Multiple format string vulnerabilities in the tolog function in httpdx 1.4, 1.4.5, 1.4.6, 1.4.6b, and 1.5 allow (1) remote attackers to execute arbitrary code via format string specifiers in a GET request to the HTTP server component when logging is enabled, and allow (2) remote authenticated users to execute arbitrary code via format string specifiers in a PWD command to the FTP server component.

CVE-2009-4769 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 9.3 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit	Exploit, www.metasploit.com, text/html, Inactive Link, Not Archived	MISC www.metasploit.com/redmine/projects/framework/repository/revisions/7569/entry/module
No Description Provided	osvdb.org, Inactive Link, Not Archived	OSVDB 60181
Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit	Exploit, www.metasploit.com, text/html, Inactive Link, Not Archived	MISC www.metasploit.com/redmine/projects/framework/repository/revisions/7569/entry/module

No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 60182
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-3312

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	Jasper	Httpdx	1.4	All	All	All
Application	Jasper	Httpdx	1.4.5	All	All	All
Application	Jasper	Httpdx	1.4.6	All	All	All
Application	Jasper	Httpdx	1.4.6b	All	All	All
Application	Jasper	Httpdx	1.5	All	All	All
Application	Jasper	Httpdx	1.4	All	All	All
Application	Jasper	Httpdx	1.4.5	All	All	All
Application	Jasper	Httpdx	1.4.6	All	All	All
Application	Jasper	Httpdx	1.4.6b	All	All	All
Application	Jasper	Httpdx	1.5	All	All	All

cpe:2.3:a:jasper:httpdx:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.4.5:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.4.6:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.4.6b:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.4.5:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.4.6:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.4.6b:*:*:*:*:*:*:*:

cpe:2.3:a:jasper:httpdx:1.5:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→