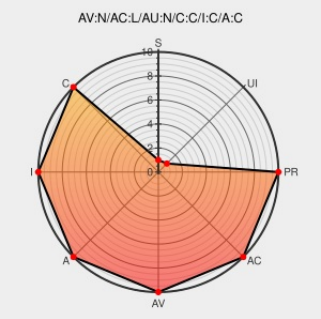
CVE-2009-3711

Published on: 10/16/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:24 PM UTC

CVE-2009-3711

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



Certain versions of Httpdx from Jasper contain the following vulnerability:

Stack-based buffer overflow in the h_handlepeer function in http.cpp in httpdx 1.4, and possibly 1.4.3, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long HTTP GET request.

CVE-2009-3711 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
No Description Provided	osvdb.org Inactive Link Not Archived	OSVDB 58714
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20091009 Re: Remote buffer overflow in httpdx
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	Vendor Advisory www.vupen.com text/html	VUPEN ADV-2009-2874
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF httpdx-hhandlepeer-bo(53700)
httpdx 1.4 GET Request Remote Buffer Overflow Exploit (0day)	Exploit www.pank4j.com text/x-c	MISC www.pank4j.com/exploits/httpdxb0f.php

	Inactive Link Not Archived	
httpdx "h_handlepeer()" Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 36991
SecurityFocus	www.securityfocus.com text/x-c	BUGTRAQ 20091008 Remote buffer overflow in httpdx
'Re: Re: Remote buffer overflow in httpdx' - MARC	Exploit marc.info text/html	BUGTRAQ 20091010 marc.info/?l=bugtraq&m=125544914512291&w=2

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	1.4.3	All	All	All
Application	Jasper	Httpdx	1.4	All	All	All
Application	Jasper	Httpdx	1.4.3	All	All	All

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

cpe:2.3:a:jasper:httpdx:1.4.3:*:*:*:*:*:*:*

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

cpe:2.3:a:jasper:httpdx:1.4.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→