



CVE-2009-3050

Published on: 09/02/2009 12:00:00 AM UTC

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

CVE-2009-3050

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Buffer overflow in the `set_page_size` function in `util.cxx` in HTMLDOC 1.8.27 and earlier allows context-dependent attackers to execute arbitrary code via a long MEDIA SIZE comment. NOTE: it was later reported that there were additional vectors in `htmllib.cxx` and `ps-pdf.cxx` using an AFM font file with a long glyph name, but these vectors do not cross privilege boundaries.

CVE-2009-3050 has been assigned by [M](#) 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
oss-security - Re: CVE Request -- HTMLDOC	www.openwall.com text/html	MLIST [oss-security] 20090725 Re: CVE Request -- HTMLDOC
HTMLDOC "set_page_size()" Buffer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 35780
Files ≈ Packet Storm	Exploit packetstormsecurity.org text/x-perl	MISC packetstormsecurity.org/0907-exploits/htmldoc-overflow.txt
oss-security - Re: CVE Request -- HTMLDOC	www.openwall.com text/html	MLIST [oss-security] 20090901 Re: CVE Request -- HTMLDOC

No Description Provided	Exploit www.htmldoc.org inode/x-empty	CONFIRM www.htmldoc.org/str.php?L214
oss-security - Re: CVE Request -- HTMLDOC	www.openwall.com text/html	MLIST [oss-security] 20090726 Re: CVE Request -- HTMLDOC
Gentoo Bug 278186 -	Exploit bugs.gentoo.org text/html	CONFIRM bugs.gentoo.org/show_bug.cgi?id=278186

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	Htmldoc	Htmldoc	1.8.24	All	All	All
Application	Htmldoc	Htmldoc	1.8.25	All	All	All
Application	Htmldoc	Htmldoc	1.8.26	All	All	All
Application	Htmldoc	Htmldoc	1.8.24	All	All	All
Application	Htmldoc	Htmldoc	1.8.25	All	All	All
Application	Htmldoc	Htmldoc	1.8.26	All	All	All
Application	Htmldoc	Htmldoc	All	All	All	All
cpe:2.3:a:htmldoc:htmldoc:1.8.24:*:*:*:*:*:						
cpe:2.3:a:htmldoc:htmldoc:1.8.25:*:*:*:*:*:						
cpe:2.3:a:htmldoc:htmldoc:1.8.26:*:*:*:*:*:						
cpe:2.3:a:htmldoc:htmldoc:1.8.24:*:*:*:*:*:						
cpe:2.3:a:htmldoc:htmldoc:1.8.25:*:*:*:*:*:						
cpe:2.3:a:htmldoc:htmldoc:1.8.26:*:*:*:*:*:						
cpe:2.3:a:htmldoc:htmldoc:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)