



CVE-2006-4256

Published on: 08/21/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:56 PM UTC

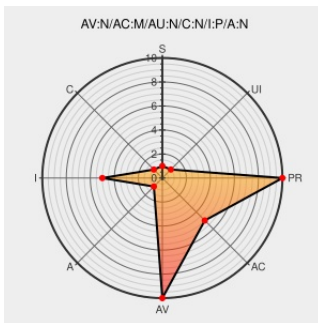
CVE-2006-4256

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Application Framework](#) from [Horde](#) contain the following vulnerability:

index.php in Horde Application Framework before 3.1.2 allows remote attackers to include web pages from other sites, which could be useful for phishing attacks, via a URL in the url parameter, aka "cross-site referencing." NOTE: some sources have referred to this issue as XSS, but it is different than classic XSS.

CVE-2006-4256 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
SecurityReason - Horde Framework and Horde IMP /index.php cross site referencing	securityreason.com text/html	SREASON 1422
[announce] Horde 3.1.3 (final)	lists.horde.org text/html	MLIST [horde-announce] 20060817 Horde 3.1.3 (final)
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060816 [scip_Advisory 2456] Horde Framework and Horde IMP /index.php cross site referencing
Debian update for horde3 - Advisories - Secunia	web.archive.org text/html	SECUNIA 27565
Horde Phishing and Cross-Site Scripting Vulnerabilities - Advisories -	Vendor Advisory	SECUNIA 21500

Secunia	web.archive.org text/html	
scip AG [Security - Consulting - Information - Process]	www.scip.ch text/xml	 MISC www.scip.ch/cgi-bin/smss/showadvf.pl?id=2456
SecurityTracker.com Archives - Horde Application Framework Input Validation Holes in 'index.php' and IMP's 'search.php' Permit Cross-Site Scripting Attacks	securitytracker.com text/html	 SECTrack 1016713
Webmail- OVH	www.vupen.com text/html	 VUPEN ADV-2006-3309
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF horde-index-xss(28411)
Debian -- Security Information -- DSA-1406-1 horde3	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1406

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	Horde	Application Framework	3.0	All	All	All
Application	Horde	Application Framework	3.0.1	All	All	All
Application	Horde	Application Framework	3.0.2	All	All	All
Application	Horde	Application Framework	3.0.3	All	All	All
Application	Horde	Application Framework	3.0.4	All	All	All
Application	Horde	Application Framework	3.0.4_rc1	All	All	All
Application	Horde	Application Framework	3.0.4_rc2	All	All	All
Application	Horde	Application Framework	3.0.6	All	All	All
Application	Horde	Application Framework	3.0.7	All	All	All
Application	Horde	Application Framework	3.0.8	All	All	All
Application	Horde	Application Framework	3.0.9	All	All	All
Application	Horde	Application Framework	3.1	All	All	All
Application	Horde	Application Framework	3.1.1	All	All	All
Application	Horde	Application Framework	3.0	All	All	All
Application	Horde	Application Framework	3.0.1	All	All	All
Application	Horde	Application Framework	3.0.2	All	All	All
Application	Horde	Application Framework	3.0.3	All	All	All
Application	Horde	Application Framework	3.0.4	All	All	All

Application	Vendor	Application Framework	Version	Platform	Architecture	OS
Application	Horde	Application Framework	3.0.4_rc1	All	All	All
Application	Horde	Application Framework	3.0.4_rc2	All	All	All
Application	Horde	Application Framework	3.0.6	All	All	All
Application	Horde	Application Framework	3.0.7	All	All	All
Application	Horde	Application Framework	3.0.8	All	All	All
Application	Horde	Application Framework	3.0.9	All	All	All
Application	Horde	Application Framework	3.1	All	All	All
Application	Horde	Application Framework	3.1.1	All	All	All
cpe:2.3:a:horde:application_framework:3.0:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.4:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.4_rc1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.4_rc2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.6:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.7:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.8:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.9:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.1.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.4:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.4_rc1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.4_rc2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.6:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.0.7:*:*:*:*:*:						

cpe:2.3:a:horde:application_framework:3.0.8:*****:	
cpe:2.3:a:horde:application_framework:3.0.9:*****:	
cpe:2.3:a:horde:application_framework:3.1:*****:	
cpe:2.3:a:horde:application_framework:3.1.1:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→