



CVE-2009-3236

Published on: 09/17/2009 12:00:00 AM UTC

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

CVE-2009-3236

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

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

The form library in Horde Application Framework 3.2 before 3.2.5 and 3.3 before 3.3.5; Groupware 1.1 before 1.1.6 and 1.2 before 1.2.4; and Groupware Webmail Edition 1.1 before 1.1.6 and 1.2 before 1.2.4; reuses temporary filenames during the upload process which allows remote attackers, with privileges to write to the address book, to

overwrite arbitrary files and execute PHP code via crafted Horde_Form_Type_image form field elements.

CVE-2009-3236 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Debian update for horde3 - Secunia Advisories - Vulnerability Information - Secunia.com

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[X SECUNIA 36882](#)

Debian -- Security Information -- DSA-1897-1 horde3

[www.debian.org](#)
[Deprecated Link](#)
[text/html](#)

[DEBIAN DSA-1897](#)

'[announce] [SECURITY] Horde 3.2.5 (final)' - MARC

[Patch](#)
[marc.info](#)
[text/html](#)

[MLIST \[horde-announce\] 20090914 \[announce\] \[SECURITY\] Horde 3.2.5 \(final\)](#)

'[announce] [SECURITY] Horde 3.3.5 (final)' - MARC	Patch marc.info text/html	MLIST [horde-announce] 20090914 [announce] [SECURITY] Horde 3.3.5 (final)
No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 58107
Horde Application Framework Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	Vendor Advisory web.archive.org text/html	SECUNIA 36665
'[announce] Horde Groupware 1.2.4 (final)' - MARC	Patch marc.info text/html	MLIST [horde-announce] 20090914 [announce] Horde Groupware 1.2.4 (final)
'[announce] Horde Groupware Webmail Edition 1.2.4 (final)' - MARC	Patch marc.info text/html	MLIST [horde-announce] 20090914 [announce] Horde Groupware Webmail Edition 1.2.4 (final)
'[announce] Horde Groupware 1.1.6 (final)' - MARC	Patch marc.info text/html	MLIST [horde-announce] 20090914 [announce] Horde Groupware 1.1.6 (final)
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF horde-application-form-file-overwrite(53202)
'[announce] Horde Groupware Webmail Edition 1.1.6 (final)' - MARC	Patch marc.info text/html	MLIST [horde-announce] 20090914 [announce] Horde Groupware Webmail Edition 1.1.6 (final)

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	3.2	All	All	All
Application	Horde	Application Framework	3.2.1	All	All	All
Application	Horde	Application Framework	3.2.2	All	All	All
Application	Horde	Application Framework	3.2.3	All	All	All
Application	Horde	Application Framework	3.2.4	All	All	All
Application	Horde	Application Framework	3.3	All	All	All
Application	Horde	Application Framework	3.3.1	All	All	All
Application	Horde	Application Framework	3.3.2	All	All	All
Application	Horde	Application Framework	3.3.3	All	All	All
Application	Horde	Application Framework	3.3.4	All	All	All
Application	Horde	Application Framework	3.2	All	All	All
Application	Horde	Application Framework	3.2.1	All	All	All

Application	Horde	Application Framework	3.2.2	All	All	All
Application	Horde	Application Framework	3.2.3	All	All	All
Application	Horde	Application Framework	3.2.4	All	All	All
Application	Horde	Application Framework	3.3	All	All	All
Application	Horde	Application Framework	3.3.1	All	All	All
Application	Horde	Application Framework	3.3.2	All	All	All
Application	Horde	Application Framework	3.3.3	All	All	All
Application	Horde	Application Framework	3.3.4	All	All	All
Application	Horde	Groupware	1.1	All	All	All
Application	Horde	Groupware	1.1	rc1	All	All
Application	Horde	Groupware	1.1	rc2	All	All
Application	Horde	Groupware	1.1	rc3	All	All
Application	Horde	Groupware	1.1	rc4	All	All
Application	Horde	Groupware	1.1.1	All	All	All
Application	Horde	Groupware	1.1.2	All	All	All
Application	Horde	Groupware	1.1.3	All	All	All
Application	Horde	Groupware	1.1.4	All	All	All
Application	Horde	Groupware	1.1.5	All	All	All
Application	Horde	Groupware	1.2	All	All	All
Application	Horde	Groupware	1.2	rc1	All	All
Application	Horde	Groupware	1.2.1	All	All	All
Application	Horde	Groupware	1.2.2	All	All	All
Application	Horde	Groupware	1.2.3	All	All	All
Application	Horde	Groupware	1.2.3	rc1	All	All
Application	Horde	Groupware	1.1	All	All	All
Application	Horde	Groupware	1.1	rc1	All	All
Application	Horde	Groupware	1.1	rc2	All	All
Application	Horde	Groupware	1.1	rc3	All	All
Application	Horde	Groupware	1.1	rc4	All	All
Application	Horde	Groupware	1.1.1	All	All	All
Application	Horde	Groupware	1.1.2	All	All	All
Application	Horde	Groupware	1.1.3	All	All	All
Application	Horde	Groupware	1.1.4	All	All	All
Application	Horde	Groupware	1.1.5	All	All	All
Application	Horde	Groupware	1.2	All	All	All

Application	Horde	Groupware	1.2	rc1	All	All
Application	Horde	Groupware	1.2.1	All	All	All
Application	Horde	Groupware	1.2.2	All	All	All
Application	Horde	Groupware	1.2.3	All	All	All
Application	Horde	Groupware	1.2.3	rc1	All	All
cpe:2.3:a:horde:application_framework:3.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.4:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.4:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.2.4:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.1:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.2:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.3:*:*:*:*:*:						
cpe:2.3:a:horde:application_framework:3.3.4:*:*:*:*:*:						
cpe:2.3:a:horde:groupware:1.1:*:*:*:*:*:						
cpe:2.3:a:horde:groupware:1.1:rc1:*:*:*:*:*:						
cpe:2.3:a:horde:groupware:1.1:rc2:*:*:*:*:*:						
cpe:2.3:a:horde:groupware:1.1:rc3:*:*:*:*:*:						

cpe:2.3:a:horde:groupware:1.1:rc4:*****:
cpe:2.3:a:horde:groupware:1.1.1:*****:
cpe:2.3:a:horde:groupware:1.1.2:*****:
cpe:2.3:a:horde:groupware:1.1.3:*****:
cpe:2.3:a:horde:groupware:1.1.4:*****:
cpe:2.3:a:horde:groupware:1.1.5:*****:
cpe:2.3:a:horde:groupware:1.2:*****:
cpe:2.3:a:horde:groupware:1.2:rc1:*****:
cpe:2.3:a:horde:groupware:1.2.1:*****:
cpe:2.3:a:horde:groupware:1.2.2:*****:
cpe:2.3:a:horde:groupware:1.2.3:*****:
cpe:2.3:a:horde:groupware:1.2.3:rc1:*****:
cpe:2.3:a:horde:groupware:1.1:*****:
cpe:2.3:a:horde:groupware:1.1:rc1:*****:
cpe:2.3:a:horde:groupware:1.1:rc2:*****:
cpe:2.3:a:horde:groupware:1.1:rc3:*****:
cpe:2.3:a:horde:groupware:1.1:rc4:*****:
cpe:2.3:a:horde:groupware:1.1.1:*****:
cpe:2.3:a:horde:groupware:1.1.2:*****:
cpe:2.3:a:horde:groupware:1.1.3:*****:
cpe:2.3:a:horde:groupware:1.1.4:*****:
cpe:2.3:a:horde:groupware:1.1.5:*****:
cpe:2.3:a:horde:groupware:1.2:*****:
cpe:2.3:a:horde:groupware:1.2:rc1:*****:
cpe:2.3:a:horde:groupware:1.2.1:*****:
cpe:2.3:a:horde:groupware:1.2.2:*****:
cpe:2.3:a:horde:groupware:1.2.3:*****:
cpe:2.3:a:horde:groupware:1.2.3:rc1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023  |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)