



CVE-2012-5565

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2012-5565
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-05 21:55:00 UTC
Updated	2014-04-07 15:36:00 UTC
Description	Cross-site scripting (XSS) vulnerability in js/compose-dimp.js in Horde Internet Mail Program (IMP) before 5.0.24, as used i

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Horde	Groupware	4.0	All	webamail	All
Application	Horde	Groupware	4.0	rc1	webamail	All
Application	Horde	Groupware	4.0	rc2	webamail	All
Application	Horde	Groupware	4.0.1	All	webamail	All
Application	Horde	Groupware	4.0.2	All	webamail	All
Application	Horde	Groupware	4.0.3	All	webamail	All
Application	Horde	Groupware	4.0.4	All	webamail	All
Application	Horde	Groupware	4.0.5	All	webamail	All
Application	Horde	Groupware	4.0.6	All	webamail	All
Application	Horde	Groupware	4.0.7	All	webamail	All
Application	Horde	Groupware	4.0	All	webamail	All
Application	Horde	Groupware	4.0	rc1	webamail	All
Application	Horde	Groupware	4.0	rc2	webamail	All
Application	Horde	Groupware	4.0.1	All	webamail	All
Application	Horde	Groupware	4.0.2	All	webamail	All
Application	Horde	Groupware	4.0.3	All	webamail	All
Application	Horde	Groupware	4.0.4	All	webamail	All

Application	Horde	Groupware	4.0.5	All	webmail	All
Application	Horde	Groupware	4.0.6	All	webmail	All
Application	Horde	Groupware	4.0.7	All	webmail	All
Application	Horde	Groupware	All	All	webmail	All
Application	Horde	Imp	5.0.10	All	All	All
Application	Horde	Imp	5.0.11	All	All	All
Application	Horde	Imp	5.0.12	All	All	All
Application	Horde	Imp	5.0.13	All	All	All
Application	Horde	Imp	5.0.14	All	All	All
Application	Horde	Imp	5.0.15	All	All	All
Application	Horde	Imp	5.0.16	All	All	All
Application	Horde	Imp	5.0.17	All	All	All
Application	Horde	Imp	5.0.18	All	All	All
Application	Horde	Imp	5.0.19	All	All	All
Application	Horde	Imp	5.0.20	All	All	All
Application	Horde	Imp	5.0.21	All	All	All
Application	Horde	Imp	5.0.22	All	All	All
Application	Horde	Imp	5.0.4	All	All	All
Application	Horde	Imp	5.0.5	All	All	All
Application	Horde	Imp	5.0.6	All	All	All
Application	Horde	Imp	5.0.7	All	All	All
Application	Horde	Imp	5.0.8	All	All	All
Application	Horde	Imp	5.0.9	All	All	All
Application	Horde	Imp	5.0.10	All	All	All
Application	Horde	Imp	5.0.11	All	All	All
Application	Horde	Imp	5.0.12	All	All	All
Application	Horde	Imp	5.0.13	All	All	All
Application	Horde	Imp	5.0.14	All	All	All
Application	Horde	Imp	5.0.15	All	All	All
Application	Horde	Imp	5.0.16	All	All	All
Application	Horde	Imp	5.0.17	All	All	All
Application	Horde	Imp	5.0.18	All	All	All
Application	Horde	Imp	5.0.19	All	All	All
Application	Horde	Imp	5.0.20	All	All	All
Application	Horde	Imp	5.0.21	All	All	All

Application	Horde	Imp	5.0.22	All	All	All
Application	Horde	Imp	5.0.4	All	All	All
Application	Horde	Imp	5.0.5	All	All	All
Application	Horde	Imp	5.0.6	All	All	All
Application	Horde	Imp	5.0.7	All	All	All
Application	Horde	Imp	5.0.8	All	All	All
Application	Horde	Imp	5.0.9	All	All	All
Application	Horde	Imp	All	All	All	All

References

Reference	Source	Link
[mms] SECURITY: Fix obscure XSS issue if uploading a file in dynamic ... · horde/horde@1550c6e · GitHub	CONFIRM	github.com
oss-security - Re: CVE Request -- (Horde) IMP (prior v5.0.24-git): Obscure XSS issue when uploading attachments.	MLIST	www.open
[announce] IMP H4 (5.0.24) (final)	MLIST	lists.horde
openSUSE-SU-2012:1626-1: moderate: update for horde4-imp	SUSE	lists.open
[announce] Horde Groupware Webmail Edition 4.0.9 (final)	MLIST	lists.horde
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)