



CVE-2011-0701

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-0701
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-14 19:55:00 UTC
Updated	2017-11-22 16:05:00 UTC
Description	wp-admin/async-upload.php in the media uploader in WordPress before 3.0.5 allows remote authenticated users to read (1

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Link	Tags
Debian update for wordpress - Secunia.com	SECUNIA	secunia.com	Third Party Advisory
Malformed Request	BID	www.securityfocus.com	Third Party Advisory, VDB Entry
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Third Party Advisory
Version 3.0.5 « WordPress Codex	CONFIRM	codex.wordpress.org	Patch, Vendor Advisory
oss-security - CVE request: wordpress before 3.0.5	MLIST	openwall.com	Mailing List, Third Party Advisory
[SECURITY] Fedora 14 Update: wordpress-3.1-1.fc14	FEDORA	lists.fedoraproject.org	Third Party Advisory
Changeset 17393 – WordPress Trac	CONFIRM	core.trac.wordpress.org	Patch, Vendor Advisory
[SECURITY] Fedora 13 Update: wordpress-3.1-1.fc13	FEDORA	lists.fedoraproject.org	Third Party Advisory
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	Third Party Advisory
WordPress › WordPress 3.0.5 (and 3.1 Release Candidate 4)	CONFIRM	www.wordpress.org	Patch, Vendor Advisory
Debian -- Security Information -- DSA-2190-1 wordpress	DEBIAN	www.debian.org	Third Party Advisory
[SECURITY] Fedora 15 Update: wordpress-3.1-1.fc15	FEDORA	lists.fedoraproject.org	Third Party Advisory
oss-security - Re: CVE request: wordpress before 3.0.5	MLIST	openwall.com	Mailing List, Third Party Advisory

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report