



# CVE-2006-0806

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

## Summary

<b>CVE</b>	CVE-2006-0806
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-02-21 02:02:00 UTC
<b>Updated</b>	2018-10-18 16:29:00 UTC
<b>Description</b>	Multiple cross-site scripting (XSS) vulnerabilities in ADOdb 4.71, as used in multiple packages such as phpESP, allow remote

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	John Lim	Adodb	4.66	All	All	All
Application	John Lim	Adodb	4.68	All	All	All
Application	John Lim	Adodb	4.70	All	All	All
Application	John Lim	Adodb	4.71	All	All	All
Application	John Lim	Adodb	4.66	All	All	All
Application	John Lim	Adodb	4.68	All	All	All
Application	John Lim	Adodb	4.70	All	All	All
Application	John Lim	Adodb	4.71	All	All	All

## References

Reference	Source	Link	Tags
ADODB Cross-Site Scripting Vulnerabilities - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor /
Debian update for cacti - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor /
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
Debian -- Security Information -- DSA-1029-1 libphp-adodb	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
SourceForge.net: Files	CONFIRM	<a href="http://sourceforge.net">sourceforge.net</a>	
Contact Support	MISC	<a href="http://www.gulftech.org">www.gulftech.org</a>	

23362	OSVDB	<a href="http://www.osvdb.org">www.osvdb.org</a>	
Debian update for moodle - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor A
CVS Info for project phpesp	MISC	<a href="http://phpesp.cvs.sourceforge.net">phpesp.cvs.sourceforge.net</a>	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>	Vendor A
Debian -- Security Information -- DSA-1031-1 cacti	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
SecurityReason	SREASON	<a href="http://securityreason.com">securityreason.com</a>	
Secunia - Advisories - Gentoo update for cacti	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor A
Debian update for libphp-adodb - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>	Vendor A
Gentoo Linux Documentation -- Cacti: Multiple vulnerabilities in included ADOdb	GENTOO	<a href="http://www.gentoo.org">www.gentoo.org</a>	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>	Vendor A
ADODB Multiple Cross-Site Scripting Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
Debian -- Security Information -- DSA-1030-1 moodle	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonica

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)