



Reference	Source	Link
WoW Roster Multiple Remote File Include Vulnerabilities	BID	www.securityfocus.com/bid/10444
WoWRoster.net • View topic - [1.7.0] Exploit found in lib/phpbb.php	MISC	www.wowroster.net/viewtopic.php?p=10444
SecurityReason - WoW Roster <= 1.5.x Remote File Include (hsList.php)	SREASON	securityreason.com/wowroster-1-5-x-remote-file-include-hslist-php/
SecurityFocus	BUGTRAQ	www.securityfocus.com/bugtraq/msg0010444.html
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com/wowroster-1-5-x-remote-file-include-hslist-php
WoWRoster File Inclusion Vulnerabilities - Advisories - Secunia	SECUNIA	secunia.com/advisories/41024
WoWRoster Include File Flaw in 'hsList.php' Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRAK	securitytracker.com/display.do?displayType=DETAILS&id=10444&cid=10444
CVE Program record	CVE.ORG	www.cve.org/CVE/nvrlist.php?id=CVE-2006-0444
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2006-0444

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](#)