



CVE-2008-4600

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

Summary

CVE	CVE-2008-4600
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-18 00:18:00 UTC
Updated	2017-09-29 01:32:00 UTC
Description	configure.php in PokerMax Poker League Tournament Script 0.13 allows remote attackers to bypass authentication and ga

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Steve Dawson	Pokermax Poker League Tournament Script	0.13	All	All	All
Application	Steve Dawson	Pokermax Poker League Tournament Script	0.13	All	All	All

References

Reference	Source
PokerMax Poker League Tournament Script Cookie Authentication Bypass Vulnerability	BID
PokerMax Pro Poker League "ValidUserAdmin" Cookie Security Bypass - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SEC
PokerMax Poker League Insecure Cookie Handling Vulnerability - SecurityReason.com	SRI
PokerMax Poker League 0.13 - Insecure Cookie Handling - PHP webapps Exploit	EXP
IBM X-Force Exchange	XF
CVE Program record	CVI
NVD vulnerability detail	NVI

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](#)