



CVE-2009-4351

Published on: 12/17/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:23 PM UTC

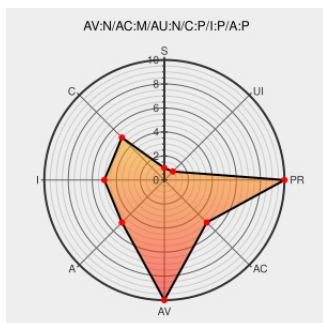
CVE-2009-4351

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Wscreeator](#) from [Wscreeator](#) contain the following vulnerability:

SQL injection vulnerability in ADMIN/loginaction.php in WSCreator 1.1, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the Email (aka username) parameter.

CVE-2009-4351 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.8 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

WSCreator 1.1 Blind SQL Injection

[Exploit](#)
[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 10446](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF wscreeator-loginaction-sql-injection\(54791\)](#)

SecurityFocus

[www.securityfocus.com](#)
[text/html](#)

[BUGTRAQ 20091215 WSCreator 1.1 Blind SQL Injection](#)

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

[Vendor Advisory](#)
[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2009-3524](#)

WSCreator "Email" SQL Injection Vulnerability - Secunia Advisories -

[Vendor Advisory](#)

[SECUNIA 37753](#)

No Description Provided

osvdb.org

OSVDB 60987

Inactive Link Not Archived

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wscreator	Wscreator	1.1	All	All	All
Application	Wscreator	Wscreator	1.1	All	All	All
cpe:2.3:a:wscreator:wscreator:1.1:*:*:*:*:*:						
cpe:2.3:a:wscreator:wscreator:1.1:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →