

[eVuln] Links Manager Multiple XSS and SQL Injection Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-09/msg00213.html>

- *From:* Alex <alex@xxxxxxxxx>
 - *Date:* Tue, 12 Sep 2006 21:02:06 +0400
-

New eVuln Advisory:
Links Manager Multiple XSS and SQL Injection Vulnerabilities
<http://evuln.com/vulns/136/summary.html>

-----Summary-----

eVuln ID: EV0136
CVE: CVE-2006-4327 CVE-2006-4328
Vendor: CloudNine Interactive
Vendor's Web Site: <http://www.cloudnineinteractive.co.uk/>
Software: Links Manager
Software's Web Site:
<http://www.cloudnineinteractive.co.uk/stuffforyou.htm>
Versions: 2006-06-12
Critical Level: Moderate
Type: Multiple Vulnerabilities
Class: Remote
Status: Unpatched. No reply from developer(s)
PoC/Exploit: Available
Solution: Not Available
Discovered by: Aliaksandr Hartsuyeu (eVuln.com)

-----Description-----

1. SQL Injection.

Vulnerable script: admin.php

Parameter nick is not properly sanitized before being used in SQL query.
This can be used to bypass authentication or make any SQL query by injecting arbitrary SQL code.

Condition: magic_quotes_gpc = off

2. Cross-Site Scripting.

Vulnerable Script: add_url.php

Parameters title description keywords are not properly sanitized. This

[eVuln] Links Manager Multiple XSS and SQL Injection Vulnerabilities

can be used to post arbitrary HTML or web script code. This code will be executed when administrator will visit control panel for link approval.

-----PoC/Exploit-----

Available at: <http://evuln.com/vulns/136/exploit.html>

-----Solution-----

No Patch available.

-----Credit-----

Discovered by: Aliaksandr Hartsuyeu (eVuln.com)

Regards,
Aliaksandr Hartsuyeu
<http://evuln.com> – Penetration Testing Services

..