

[KAPDA::#32] – d2kBlog 1.0.3 Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-03/msg00163.html>

- *From:* 3nitro@xxxxxxxxxx
 - *Date:* 8 Mar 2006 16:55:13 -0000
-

KAPDA New advisory

Vulnerable products : d2kBlog <= 1.0.3
Vendor: <http://www.d2ksoft.com/>
Risk: Medium
Vulnerabilities: SQL_Injection , Script Insertion

Date :

Found : 2006/01/01
Vendor Contacted : 2006/01/02
Release Date : 2006/03/08

About D2KBlog :

Free, open-sourced, full featured asp+access blog .

Vulnerability:

SQL_Injection:

Input passed to the "memName" parameter in 'profile.asp' via the cookie is not properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Successful exploitation extracts username and password of administrator.

Script Insertion:

Input passed to the "msg" field in 'default.asp' isn't properly sanitised before being used. This can be exploited to inject arbitrary HTML and script code, which will be executed in a user's browser session in context of an affected site when the malicious user data is viewed.

Proof of Concepts:

SQL_Injection :

Cookie : memName=[SQL_Injection]

Script Insertion :

Default.asp , POST :

name=KAPDA&email=KAPDA&msg=<script>alert("XSS")</script>&submit=Send+Message

Solution:

No patch`s released yet by vendor.
Vendor`s contacted about two months ago.

Original Advisory:

<http://www.kapda.ir/advisory-287.html>
Perl PoC : <http://www.kapda.ir/attach-1453-d2kblog.txt>

Credit :

FarhadKey of KAPDA
DevilBox of KAPDA
farhadkey [at} kapda.ir
devil_box [at} kapda.ir
Kapda – Security Science Researchers Insitute of Iran
<http://www.KAPDA.ir>