

Instantly share code, notes, and snippets.

fgimenesp / **OcoMon - Blind SQL Injection.txt** Secret

Last active last month

☆ Star

<> Code - Revisions 4

## OcoMon 4.0 - Blind SQL Injection

 **OcoMon - Blind SQL Injection.txt**

```
1 Descriptions
2
3 During the internal research I found two Unauthenticated Blind SQL Injection on OcoMon HelpDesk ap
4
5 Mitre Reference
6
7 CVE-2022-41390 and CVE-2022-41391.
8
9 Vulnerability
10
11 The vulnerability was exploited using the burpsuite and sqlmap tool:
12
13 * Sample url: http://target:8000/ocomon-4.0RC1/includes/functions/download.php?file=3134&cod=(sele
14 * Sample url: http://target:8000/ocomon-4.0RC1/includes/functions/showImg.php?file=3134&cod=(selec
15 * Vulnerable parameters: cod
16 * Type: blind sql injection
17
18 More Information
19
20 Is possible exploited this same vulnerability in other 36 endpoints:
21
22 ocomon/geral/showSelLocais.php
23 ocomon/geral/ticket_history.php
24 ocomon/geral/lendings.php:
25 admin/geral/rectories.php
26 admin/geral/units.php
27 admin/geral/mail_templates.php
28 admin/geral/appsRegistered.php
29 admin/geral/response_levels.php
30
31 admin/geral/tags.php
32 admin/geral/cat_prob3.php
```

```
32 admin/geral/messages_settings.php
33 admin/geral/cat_prob1.php
34 admin/geral/cost_centers.php
35 admin/geral/cat_prob2.php
36 admin/geral/buildings.php
37 admin/geral/status.php
38 admin/geral/domains.php
39 admin/geral/tokens.php
40 admin/geral/holidays.php
41 admin/geral/responsibility_statements.php
42 admin/geral/priorities.php:
43 admin/geral/screenprofiles.php:
44 admin/geral/mail_distribution_lists.php:
45 admin/geral/scripts_documentation.php:
46 admin/geral/departments.php:
47 invmon/geral/type_of_components.php:
48 invmon/geral/sw_softwares.php:
49 invmon/geral/sw_categories.php:
50 invmon/geral/equipments_models.php:
51 invmon/geral/warranty_times.php:
52 invmon/geral/documents.php:
53 invmon/geral/suppliers.php:
54 invmon/geral/type_of_equipments.php:
55 invmon/geral/sw_default.php:
56 invmon/geral/manufacturers.php:
57 invmon/geral/sw_licenses_types.php
58
59 Short code description
60
61 The vulnerabilty happens because the code dont have sanatization in 'cod' paramenter then is possib
62
63 Example code:
64
65 if (isset($_GET['cod'])) {
66     $query .= "WHERE dom_cod = ".$_GET['cod']."
67
68 Vendor notification
69
70 https://ocomonphp.sourceforge.io/downloads/
71
72
73
```