fgimenesp / OcoMon - Blind SQL Injection.txt

Secret

Last active last month

OcoMon 4.0 - Blind SQL Injection

OcoMon - Blind SQL Injection.txt

```
Descriptions

During the internal research I found two Unauthenticated Blind SQL Injection on OcoMon HelpDesk ap

Mitre Reference

CVE-2022-41390 and CVE-2022-41391.

Vulnerability

The vulnerability was exploited using the burpsuite and sqlmap tool:

* Sample url: http://target:8000/ocomon-4.0RC1/includes/functions/download.php?file=3134&cod=(sele
* Sample url: http://target:8000/ocomon-4.0RC1/includes/functions/showImg.php?file=3134&cod=(selec
* Vulnerable parameters: cod
* Type: blind sql injection

More Information

Is possible exploided this same vulnerability in other 36 endpoints:

ocomon/geral/showSelLocais.php
ocomon/geral/ticket_history.php
ocomon/geral/lendings.php:
admin/geral/rectories.php
admin/geral/units.php
admin/geral/mail_templates.php
admin/geral/appsRegistered.php
admin/geral/response_levels.php

admin/geral/tags.php
admin/geral/cat_prob3.php
```

```
admin/geral/messages_settings.php
admin/geral/cat_prob1.php
admin/geral/cost_centers.php
admin/geral/cat_prob2.php
admin/geral/buildings.php
admin/geral/status.php
admin/geral/domains.php
admin/geral/tokens.php
admin/geral/holidays.php
admin/geral/responsibility_statements.php
admin/geral/priorities.php:
admin/geral/screenprofiles.php:
admin/geral/mail_distribution_lists.php:
admin/geral/scripts_documentation.php:
admin/geral/departments.php:
invmon/geral/type_of_components.php:
invmon/geral/sw_softwares.php:
invmon/geral/sw_categories.php:
invmon/geral/equipments_models.php:
invmon/geral/warranty_times.php:
invmon/geral/documents.php:
invmon/geral/suppliers.php:
invmon/geral/type_of_equipments.php:
invmon/geral/sw_default.php:
invmon/geral/manufacturers.php:
invmon/geral/sw_licenses_types.php

Short code description

The vulnerabily happens because the code dont have sanatization in 'cod' paramenter then is possib

Example code:

if (isset($_GET['cod'])) {
  $query .= "WHERE dom_cod = ".$_GET['cod']."

Vendor notification

https://ocomonphp.sourceforge.io/downloads/
```