Scan report for www.cc-emblavez.fr

Scanned on 2015-02-03 08:47:40

2 x Potential Vulnerabilities In The Web Server

Description
The web server is leaking information about which version of the web server is running. The specific version used have been looked up for known vulnerabilities and are listed below. Note though that these are just potential vulnerabilities and have not been verified.

CVSS
1.1

URL
http://www.cc-emblavez.fr/

Name
CVE-2011-4415

Match
```
Apache 2.2.3

The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.
```

URL
https://www.cc-emblavez.fr/

Name
CVE-2011-4415

Match
```
Apache 2.2.3

The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.
```

Deprecated Webserver

Description
Your webserver is out of date, you should consider to update your software.

CVSS
0

Domain
www.cc-emblavez.fr

Match
```
Server: Apache v2.2.3

Apache/2.2.3 (CentOS)
```

DNS Name Server Disclosure

Description
The name of your DNS provider/server can be resolved by sending a SOA-request to any DNS server that has your records. This is quite harmless but it can be used by an attacker who's looking to gather information about their target.

CVSS
0

Domain
www.cc-emblavez.fr

Match
`ambis-dns.com`

2 x E-Mail Enumeration

Description
Your website reveals one or several e-mail addresses. Spammers could gather these addresses and use them in spam campaigns. It may also reveal identities of your users and staff. If that's the case, advanced attackers could come to the same conclusion and use those e-mails for spear phishing, privilege escalation and other attacks. You should only reveal e-mail addresses in clear text if that's intended behaviour.

CVSS
0

URL
http://www.cc-emblavez.fr/pages/accueil.php

Match
`contact@cc-emblavez.fr`

URL
http://www.cc-emblavez.fr/pages/economie/programmes_leader.htm

Match
`s.meyer@cc-emblavez.fr`

External Resources

Description
We found the following external resource(s) on your website. They've been analyzed by a total of 41 Anti-Virus solutions for your security.

CVSS
0

URL
http://www.cc-emblavez.fr/pages/emblavez/emblavez_principale.htm

Match

```
External                                                                    Resource:
http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=5,0,0,0

<object                                classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#version=5,
0,0,0" width="550" height="400">
                <param name="movie" value="../../anim_flash/localisations_cce.swf">
                <param name="quality" value="high">
                <embed>

              </object>
```

Hosting Provider Disclosure

Description
An attacker mapping out their targets could easily retrieve the names of your hosting provider or Internet service provider. By first querying the IP-addresses resolving to your domain, through a DNS A-pointer lookup, followed by one or several DNS PTR-pointer lookups on the IP-addresses resolved. However, this is expected an behaviour and a core function of the Internet.

CVSS
0

Domain
www.cc-emblavez.fr

Match
`ambis-dns.com`

3 x HTML Comments

Description
The most common purpose for HTML comments is to store temporary code written by the developer(s) within an html document. These comments are not visible to the end user browsing the web page and can only be seen by browsing the source code of the html document itself. These snippets of developer code remain inactive until you remove the comment brackets. You might want to look this over.

CVSS
0

URL
http://www.cc-emblavez.fr/

Match
```
<!--code pour google analytics-->
```

URL
https://www.cc-emblavez.fr:8443/?cid=promo-plesk-domain

Match
```
<!--_____
_____
_____IE error page size
limitation_____
_____
_____-->
```

URL
https://www.cc-emblavez.fr/test/ssi/test.shtml?1422953726516=

Match
```
<!--#echo var="REQUEST_URI"-->
```

2 x HTTP OPTIONS-Disclosure

Description
Your webserver discloses its supported HTTP methods. This poses no threat by itself. It may however aid an attacker in finding unusual configuration.

CVSS
0

Domain
www.cc-emblavez.fr

Match
`GET,HEAD,POST,OPTIONS`

Domain
www.cc-emblavez.fr

Match
`OPTIONS, GET, HEAD, POST`

HTTP Server Version

Description
Your webserver discloses what software version it's currently running. This could aid an attacker in the process of fingerprinting what attacks they are to use against it.

CVSS
0

URL
https://www.cc-emblavez.fr/

Match
```
Server: Apache/2.2.3 (CentOS)
```