0-Day Research Disassembled

About Us

Security Researchers @ Tenable

Chris Lyne
David Wells
~~Jimi Sebree~~ Joe Bingham

tenable

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()
```


tenable

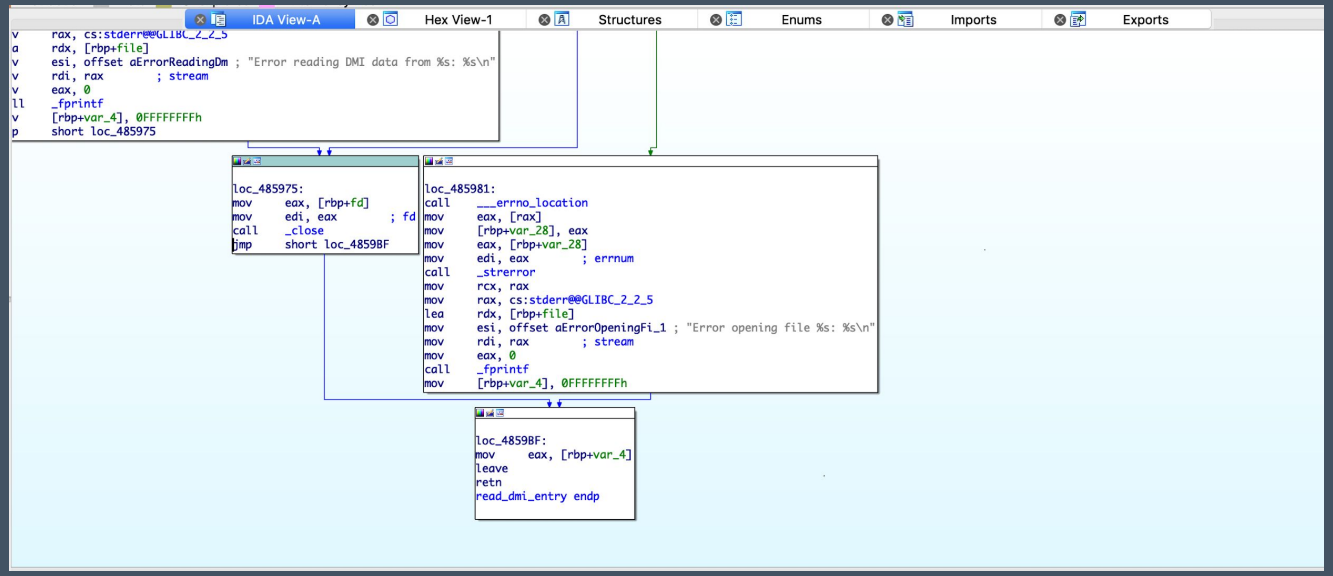
Source Code Analysis

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

```php
<?php

function get_network_info($interface) {
    $cmd = "ifconfig";

    if (!empty($interface)) {
        $cmd .= " " . $interface;
    }

    return `$cmd`;
}

echo get_network_info($_GET['interface']);

?>
```

Static Binary Analysis

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



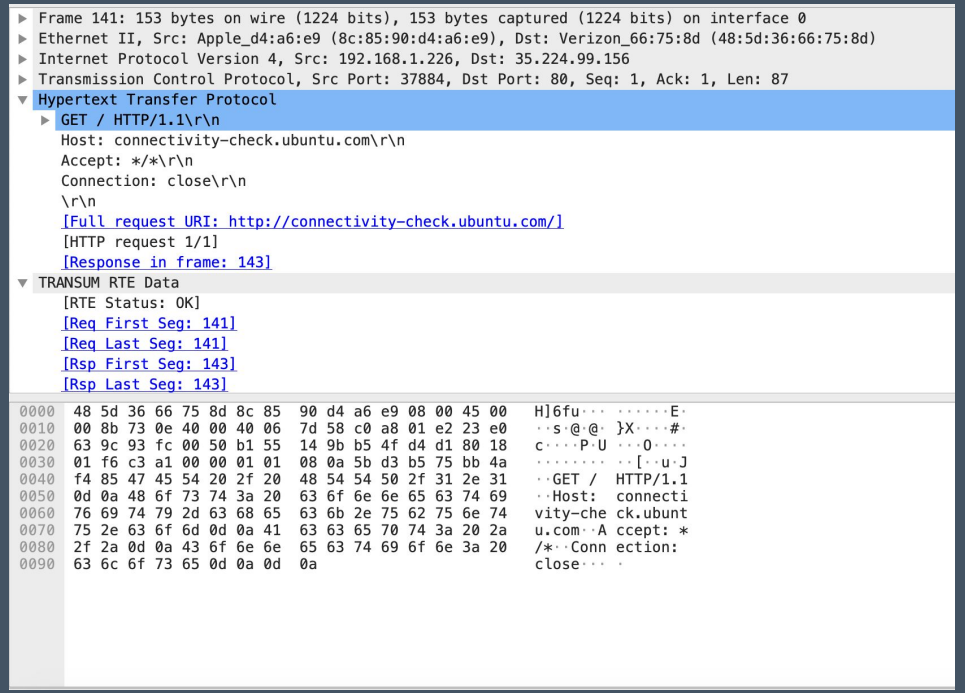
tenable

Debugging

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

Network Traffic Analysis

- Wireshark, tcpdump
- Burp Suite



tenable

Writing Tools

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

tenable

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

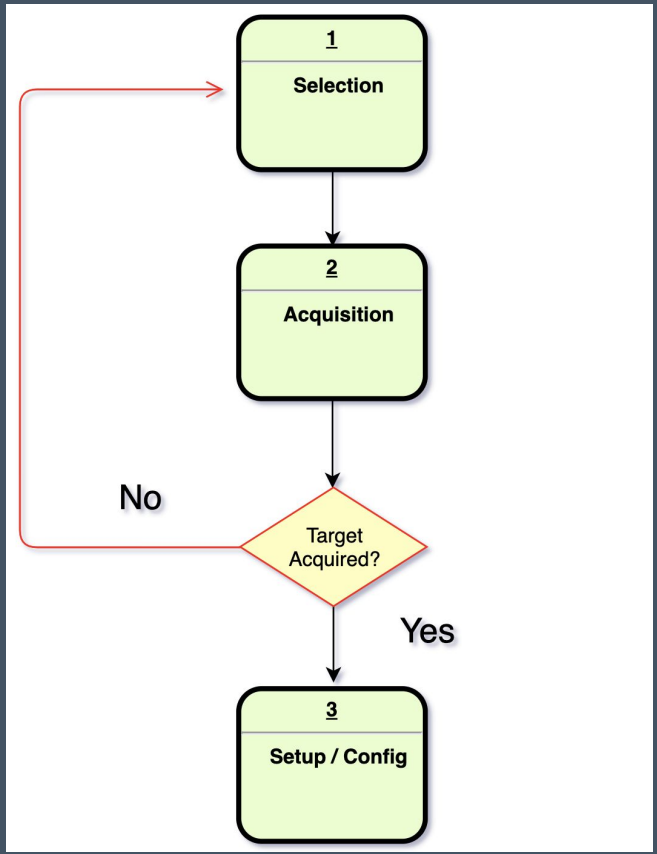
Selection

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

Goal: Produce meaningful research

Acquisition

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



tenable

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

GIF Credit: https://giphy.com/gifs/sad-panda-ALalVMOVR8Qw
Tesla: https://en.wikipedia.org/wiki/Tesla_Model_S

tenable

Try

First Name *

Last Name *

Email Address (Work) *

Phone *

Organization *

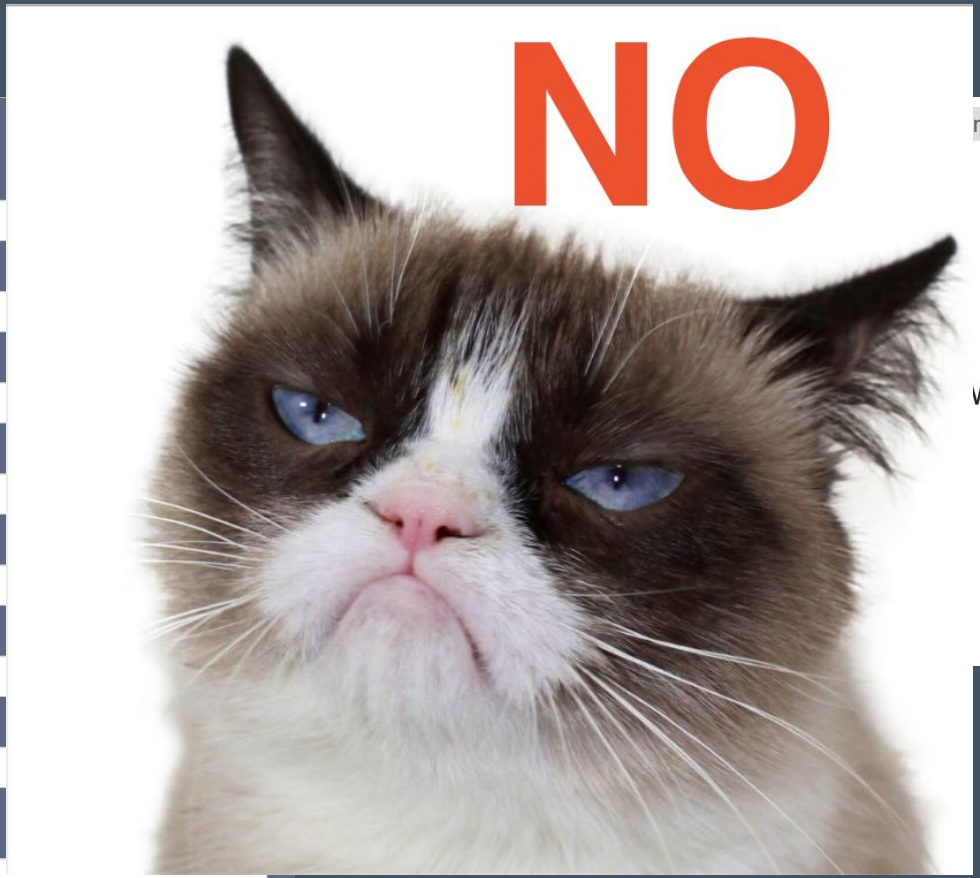
Type of Organization *

Select

Country *

Select

How can help?



nbox ×

Wed, Nov 14, 2018, 12:22 PM

What can I help you with today?

Grumpy cat: https://pbs.twimg.com/media/DyBFtEJUUAAIAZo?format=jpg&name=large

tenable

Acquisition

- Free download
- 30 day trial
- License purchased

YES!

Setup / Configuration

- Use virtual environments!
  - VMWare
  - VirtualBox
  - Docker

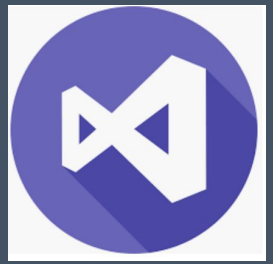
vmware

docker

tenable

Setup / Configuration

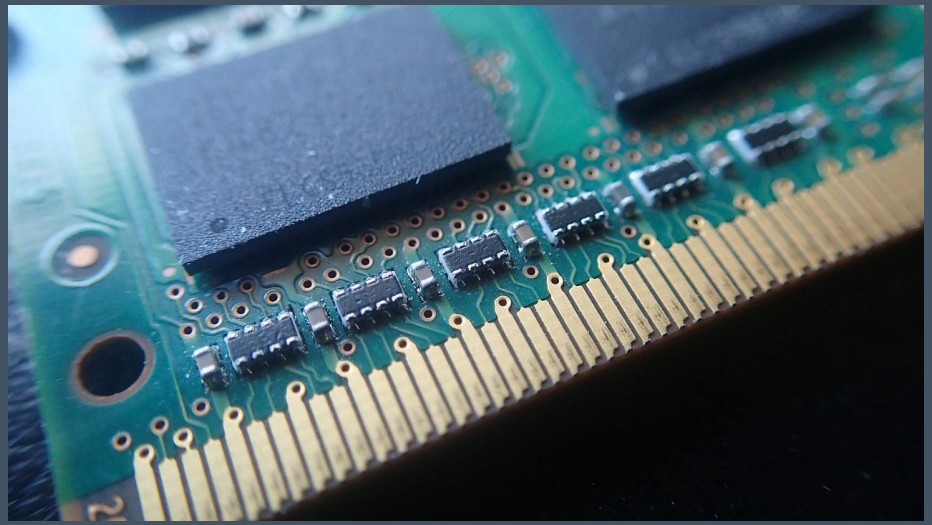
- My “base” Windows research environment (snapshot)
  - IDA Pro
  - Burp Suite
  - SysInternals tools
  - WinDbg with !exploitable plugin
  - dotPeek
  - Jd-gui
  - Visual Studio
  - Python
  - Notepad++
  - Wireshark
  - Chrome



tenable

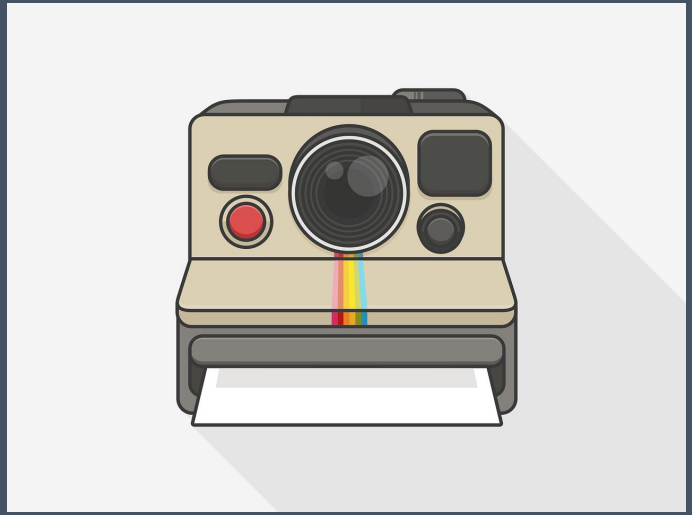
Setup / Configuration

- Install target
  - System requirements
- Dependencies



Setup / Configuration

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



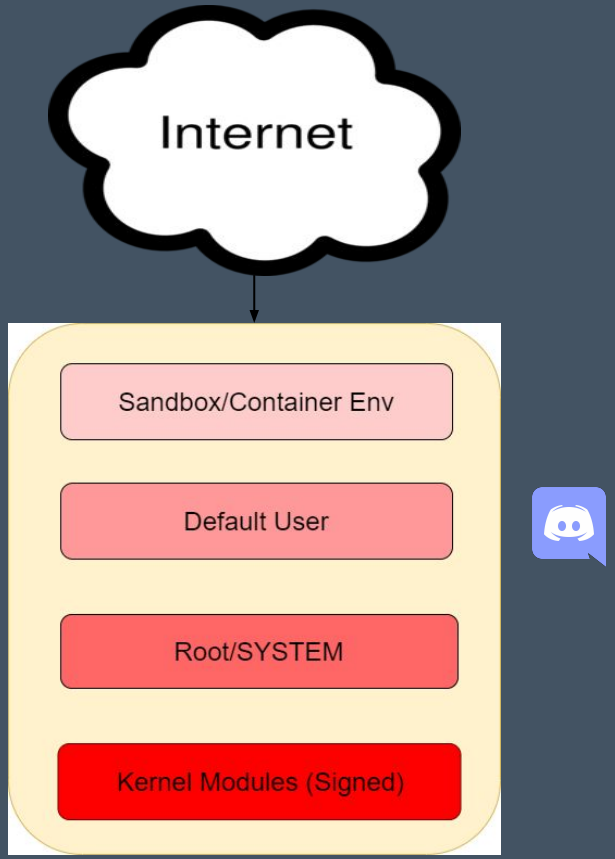
Hunting for Vulns

Finding an Attack Surface

What are the privileges of running Target?

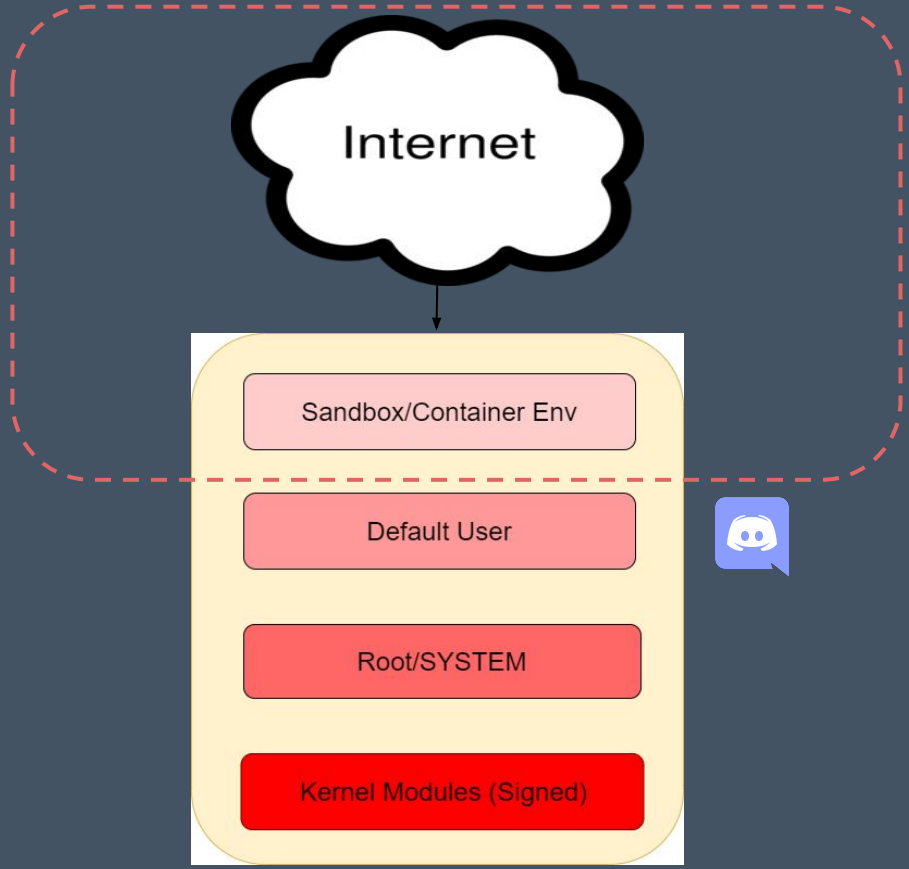
What components of the target cross into lower privilege boundaries?

Finding Attack Surface - Privilege Hierarchy



tenable

Finding Attack Surface - Attack Vector



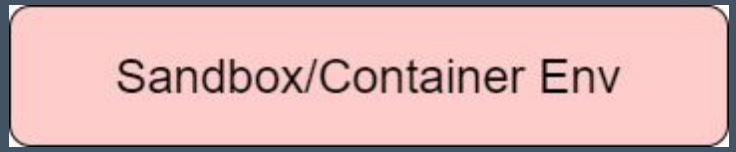
tenable

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



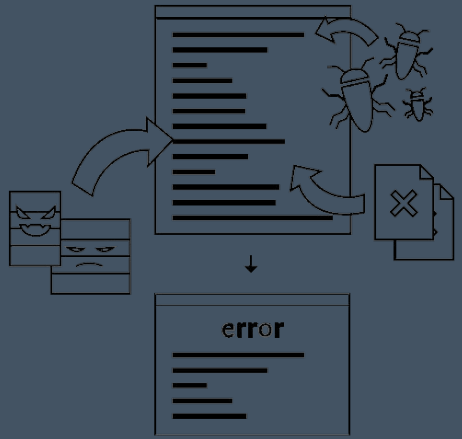
- 192.168.0.6:56732
- Hyperlink click

- 127.0.0.1:6463
- \GlobalSharedMemory_mem_*
- Hyperlink click

tenable

Component Vuln Hunting

Now that we have found an interesting Component...



Fuzzing

Disassembly

Debugging

tenable

Component Vuln Hunting

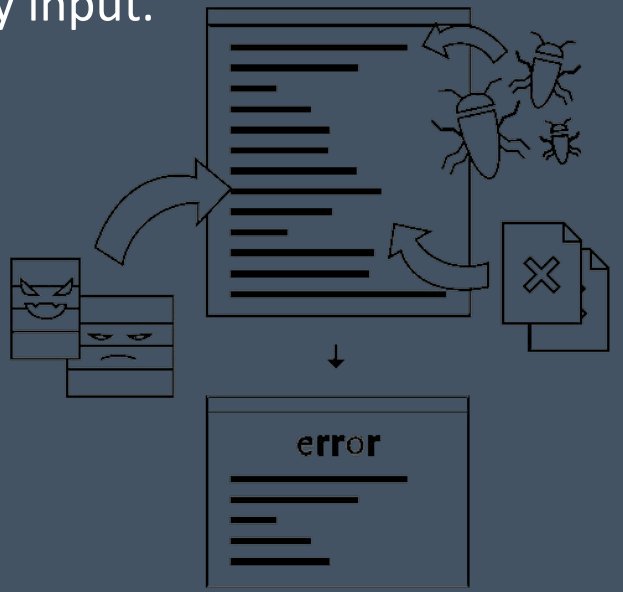
Fuzzing - Brute forcing component with arbitrary input.

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



tenable

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

tenable

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

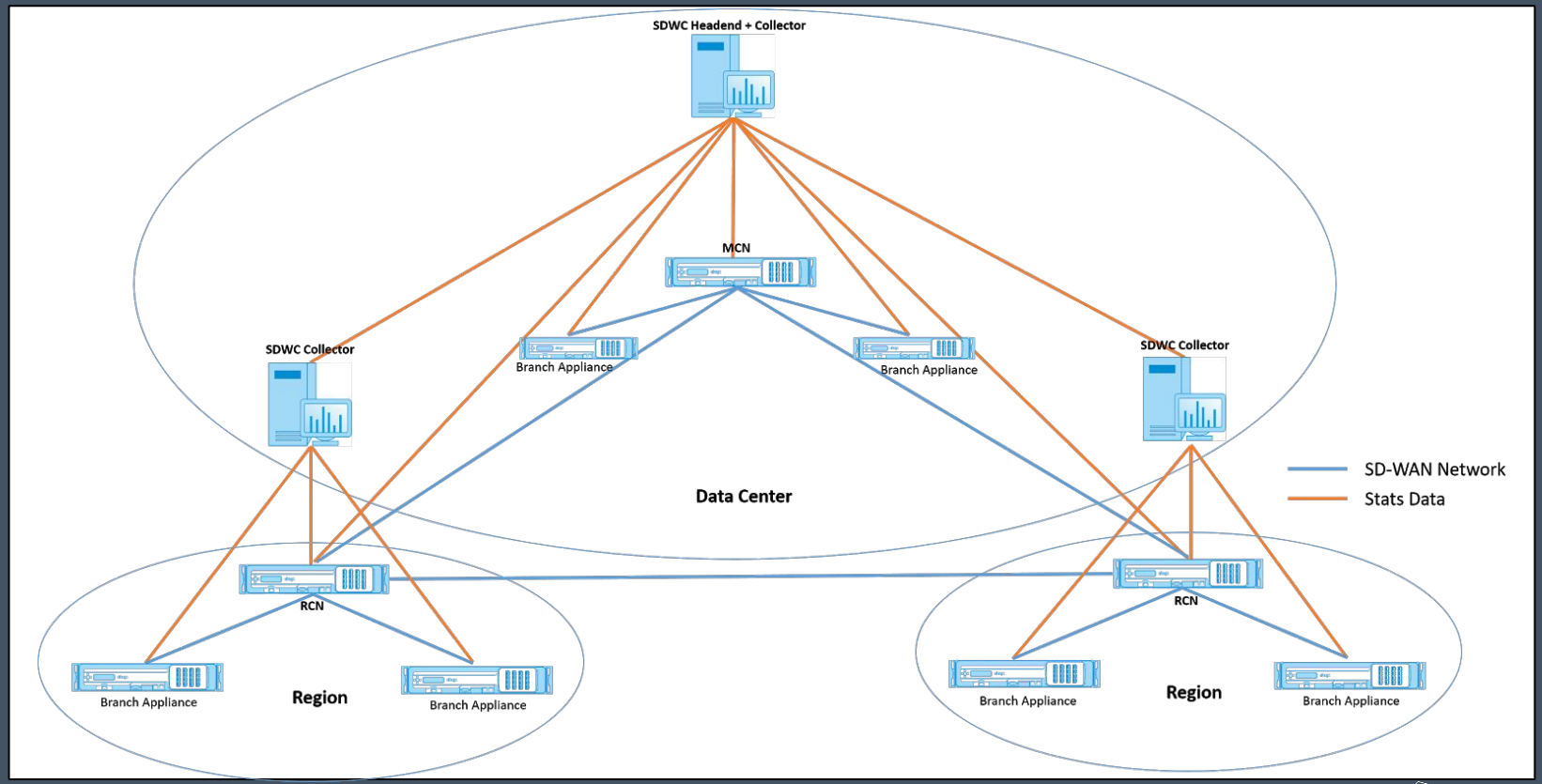
- Follow up with vendor regularly (if applicable)
- Publish findings
- Obtain bounty

Case Studies

Citrix SD-WAN

(formerly NetScaler SD-WAN)

Citrix SD-WAN



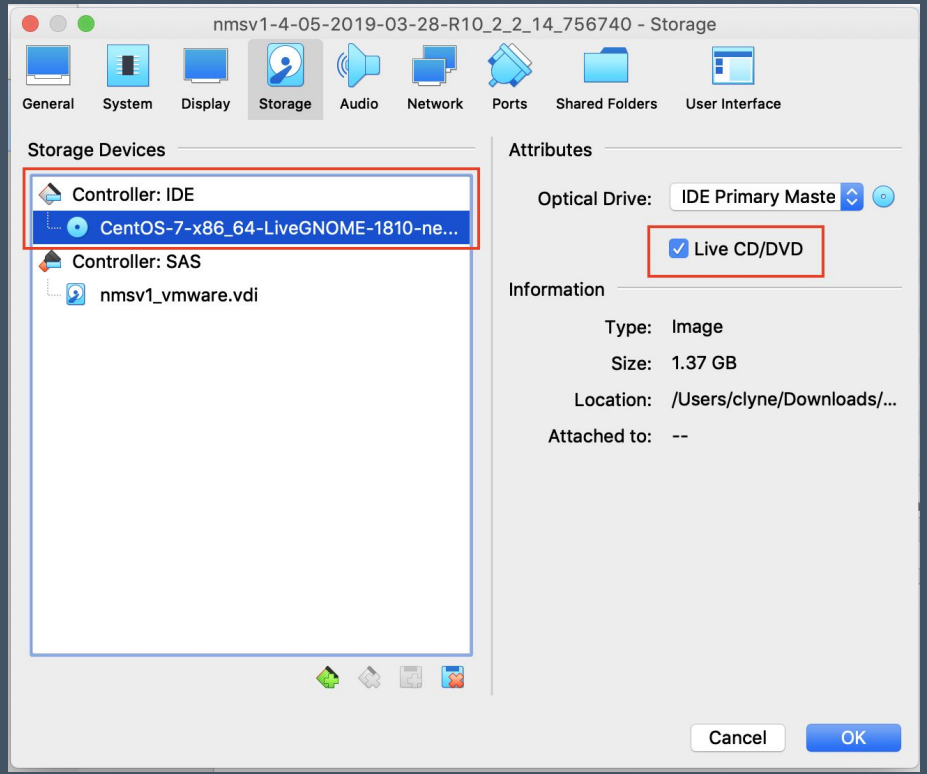
tenable

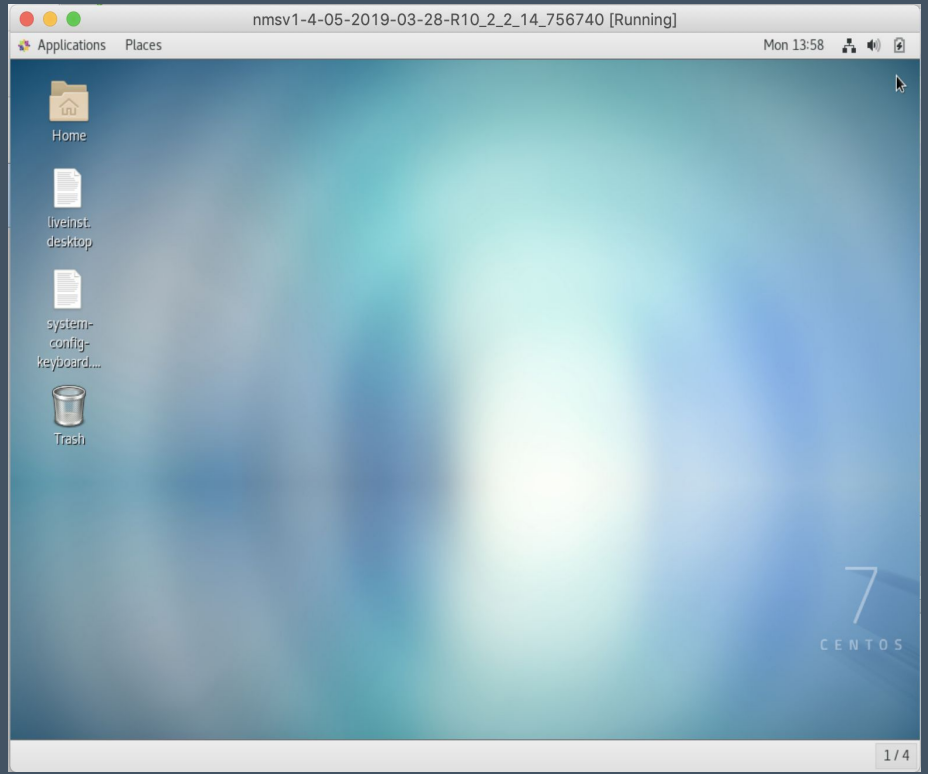
Citrix SD-WAN

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

```
sh-3.2$ 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                -
        ================================================================================================================================
```

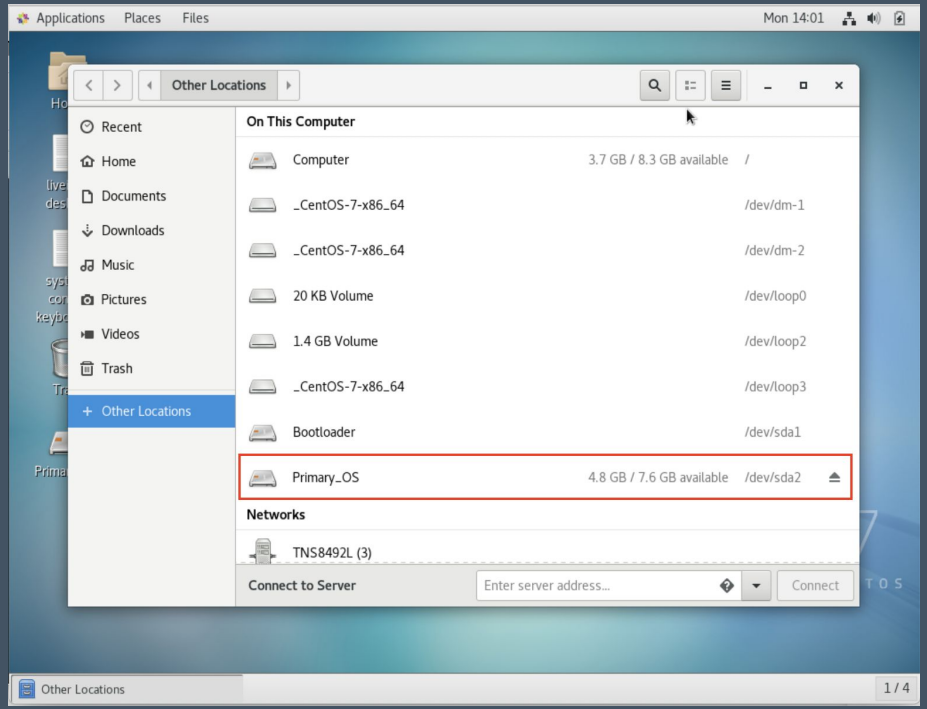
Boot from a Live CD

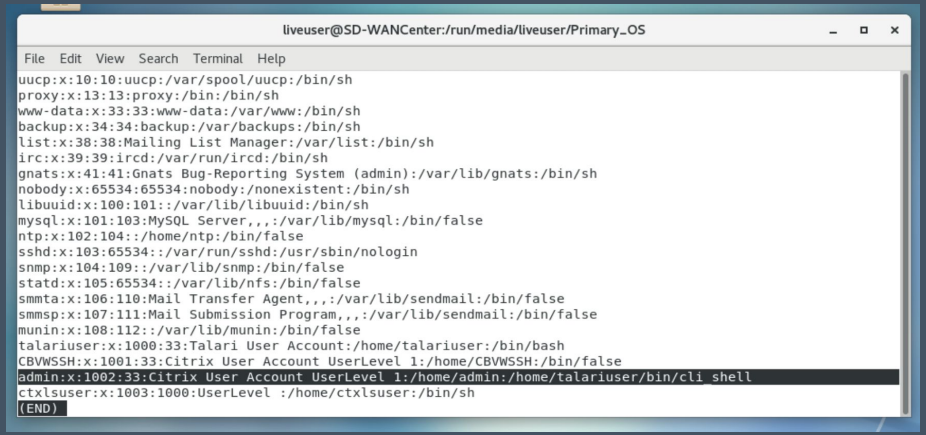




tenable

cli_shell?





tenable

Sudo!

/etc/group

/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)
```


tenable

Let’s change the shell

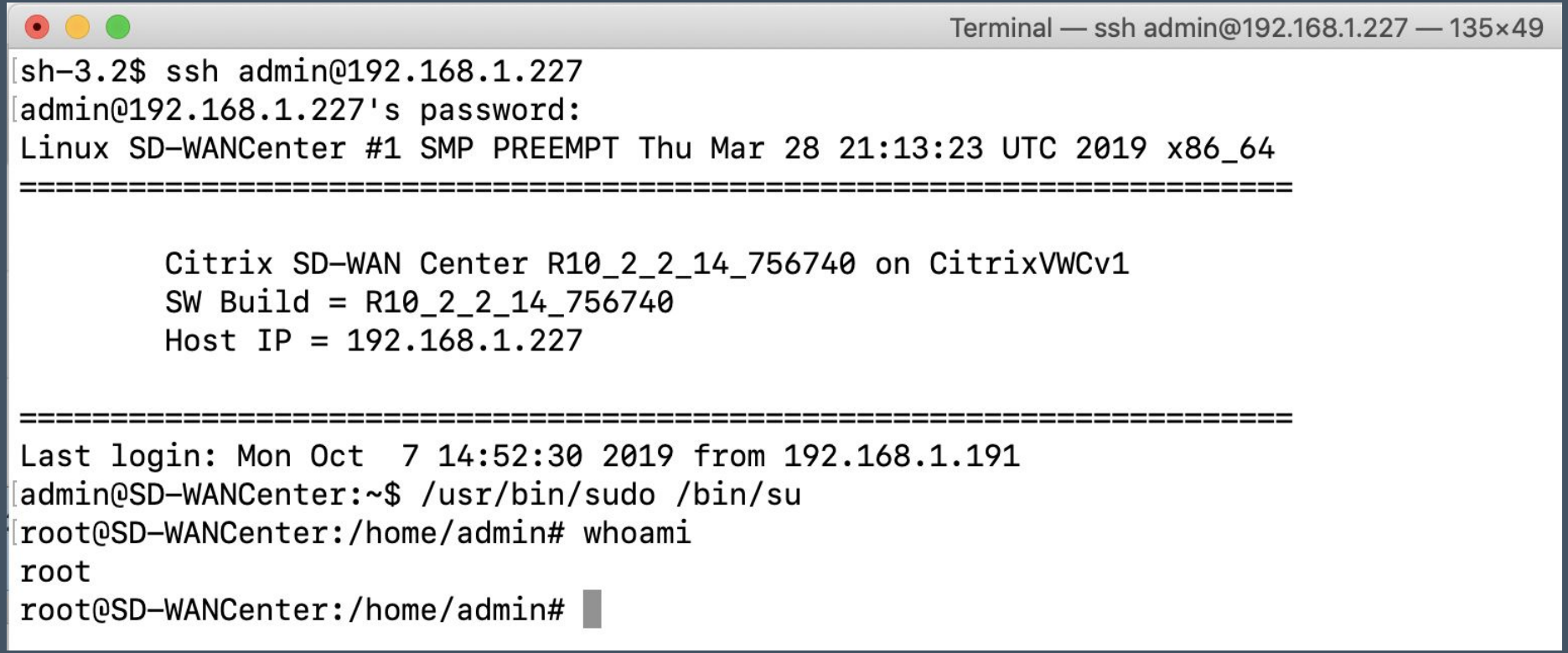
liveuser@SD-WANCenter:/run/media/liveuser/Primary_OS

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
```

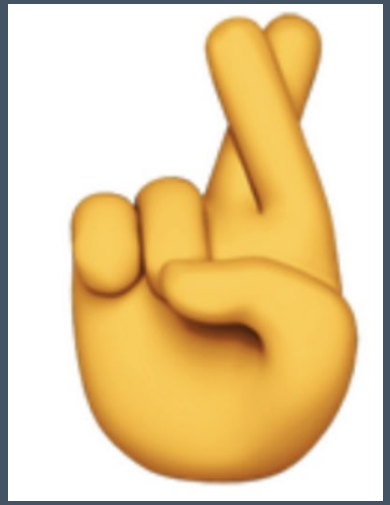

tenable

Rooted!



tenable

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

CakePHP Build fast, grow solid.

php

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

tenable

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’)

tenable

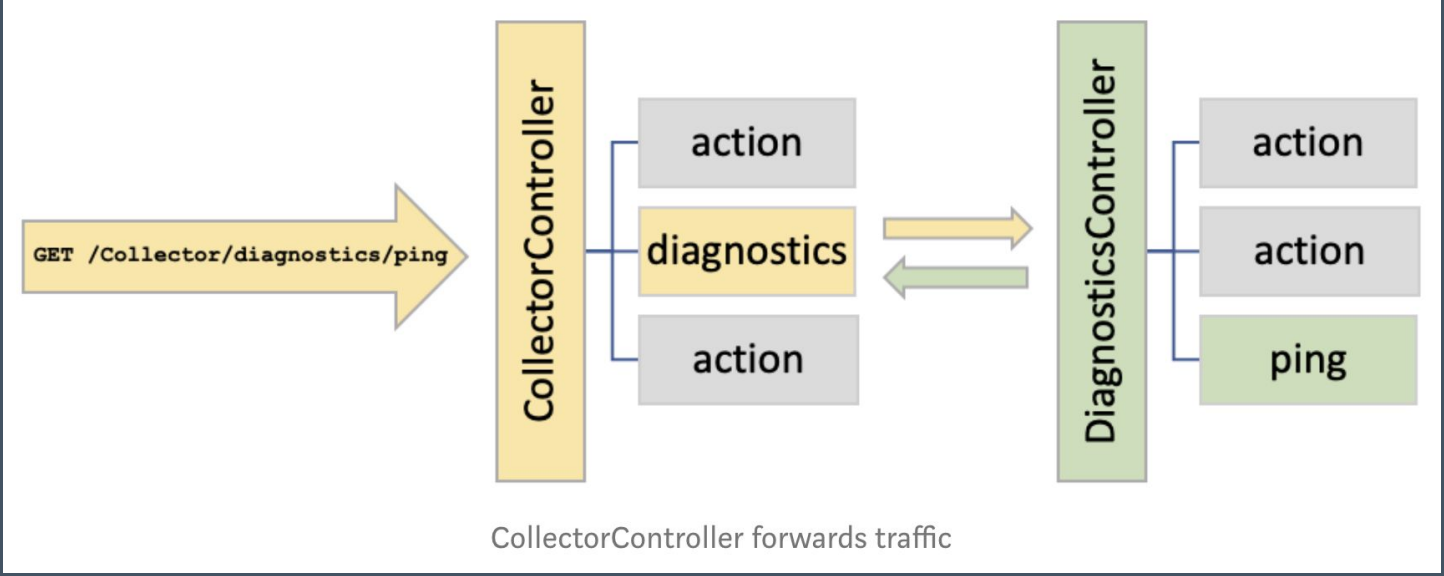
CakePHP AuthComponent

```
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('databasemgmt');
./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

tenable

Thank You, CollectorController



CollectorController forwards traffic

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

tenable

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'};
write_to_management_log("SSL Verify : $sslVerify");
# Check if we have a session - if not return error and exit
if($sslVerify eq "SUCCESS")
{
        write_to_management_log("Verified Using Certificate, dont look for login");
}else
{
        check_rest_session_and_exit_on_failure(1);
}
```

Untrusted input

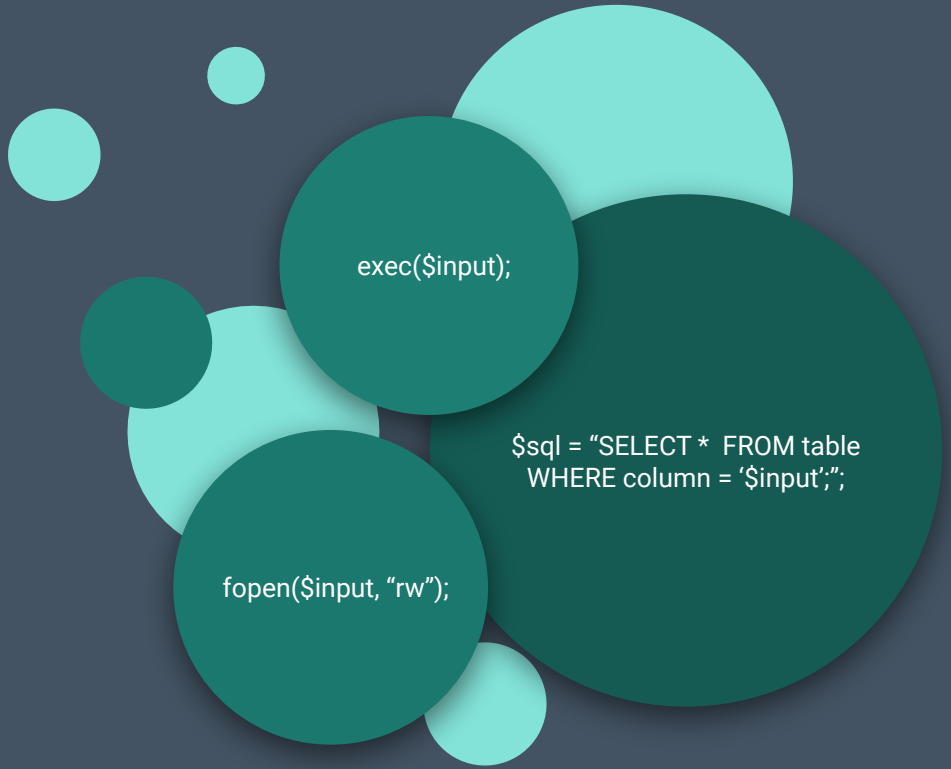
SSL_CLIENT_VERIFY : SUCCESS

Check auth

- Perl CGI
- Led to

  CVE-2019-12989

Unsafe Code Patterns



tenable

Exec All the Things!

```
root@SD-WANCenter:/home/talariuser/www/app/Controller# egrep -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);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:            $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:       $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        exec("cd " . $config_dir . $pkgName . " && " . $createTarCommand);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:        $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:            $resp = curl_exec($curl);
./ZeroTouchDeploymentController.php:       exec("cd " . $config_dir . $pkgName . " && " . $createTarCommand);
./ZeroTouchDeploymentController.php:       $resp = curl_exec($curl);
./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");
```

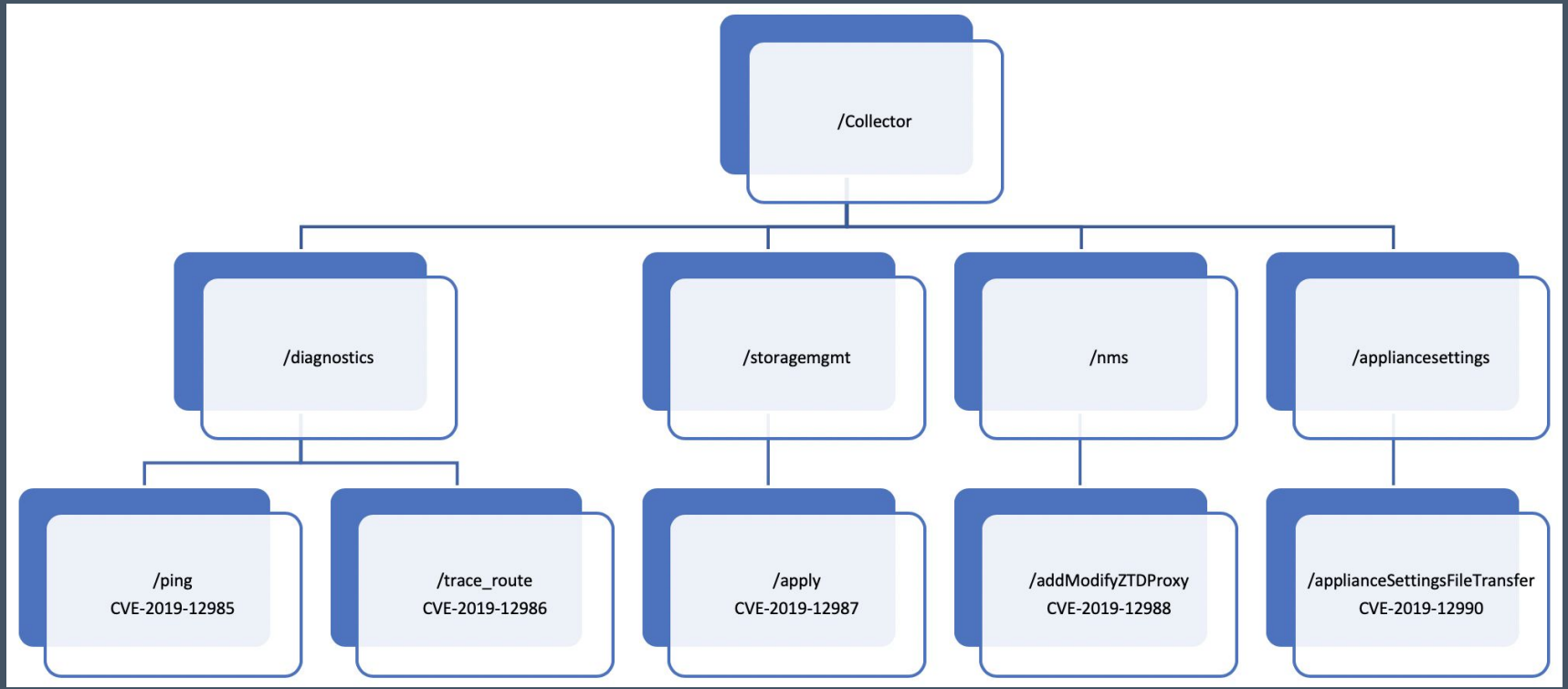
- Lots of Noise
- Tighten up regex
- Trace the untrusted input

tenable

Regex Hits for Actual Vulns

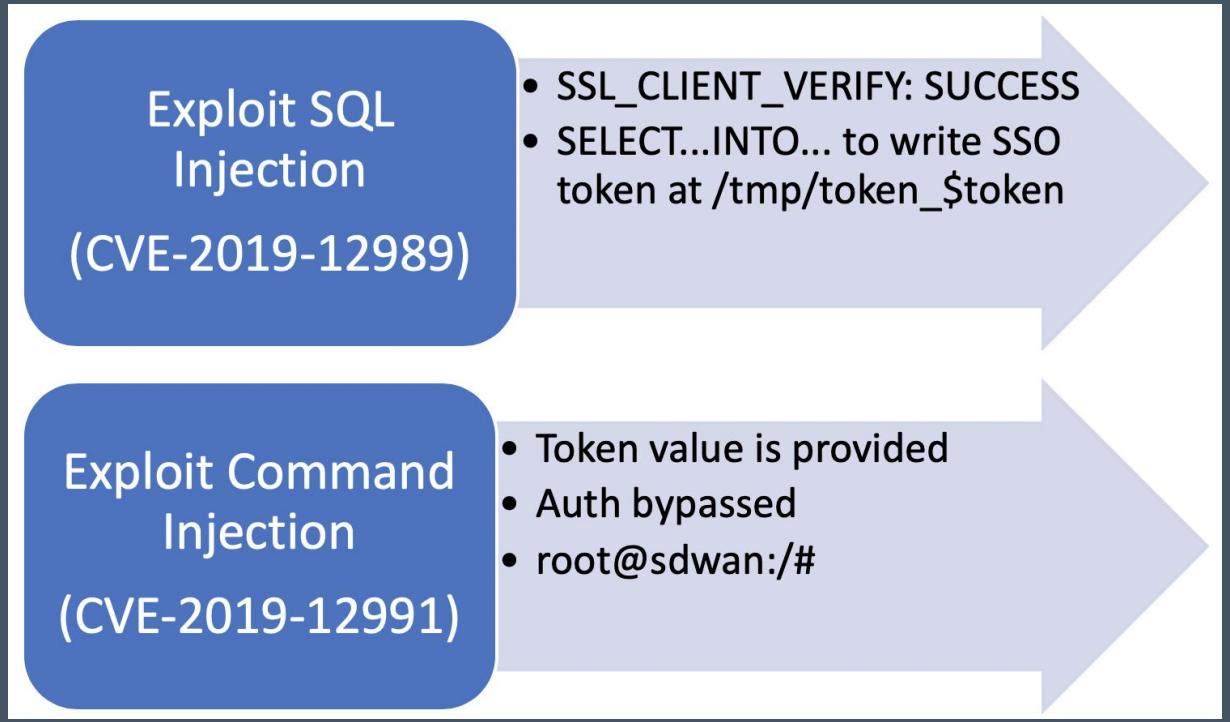
- DiagnosticsController.php: `exec(sprintf("%s > %s 2>&1 & echo $! >> %s", $cmd, $output_file, $pid_file));`
- StorageMgmtController.php: `exec("/usr/bin/perl /home/talariuser/bin/storage_mgmt.pl $action $host $path $type $migrate", $output);`
- NmsController.php: `exec($execString);`
- UsersController.php: `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



tenable

Chained Vulns for RCE in SD-WAN Appliance



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

tenable

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.

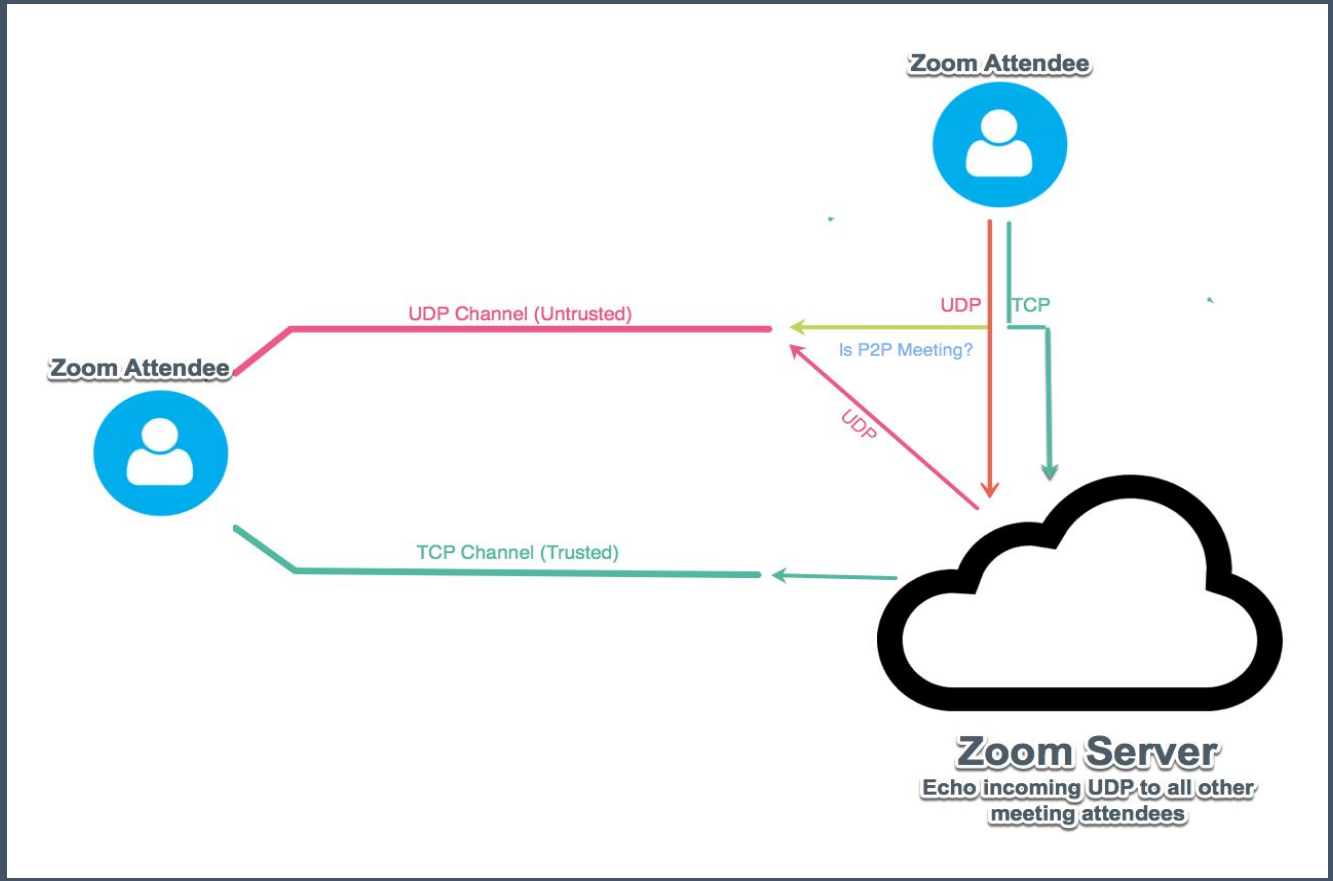
Allows attacker to spoof chat messages from other users in Zoom chat.

Allows attacker to boot other attendees from meeting.

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

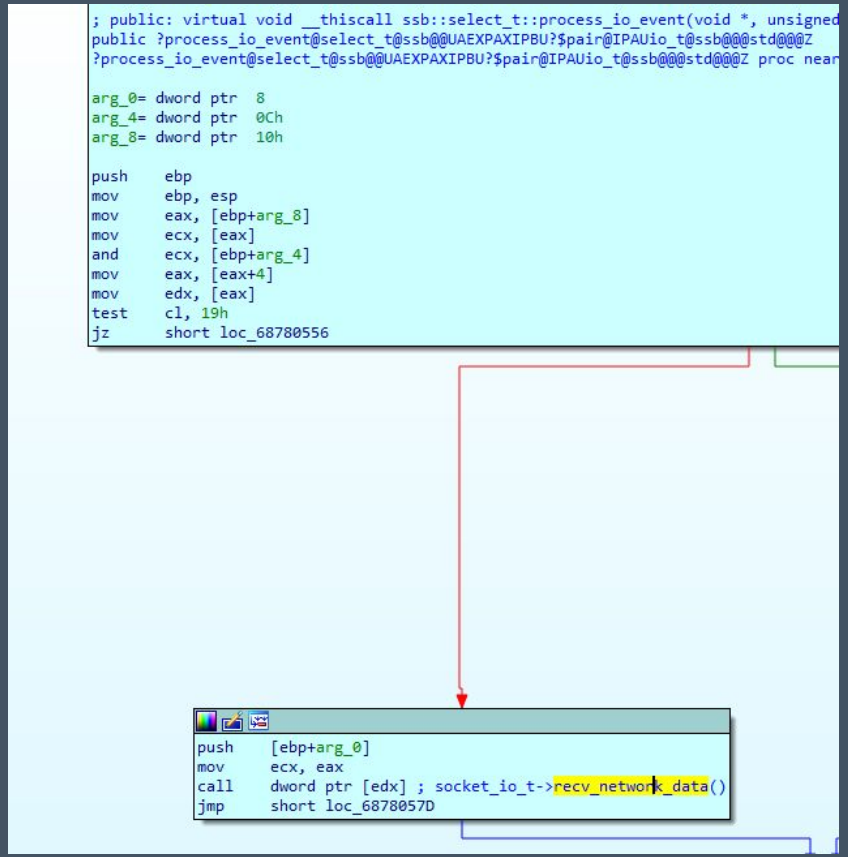
...All exploitable even by a remote non-meeting attendee

Critical Zoom Vulnerability CVE-2018-15715



tenable

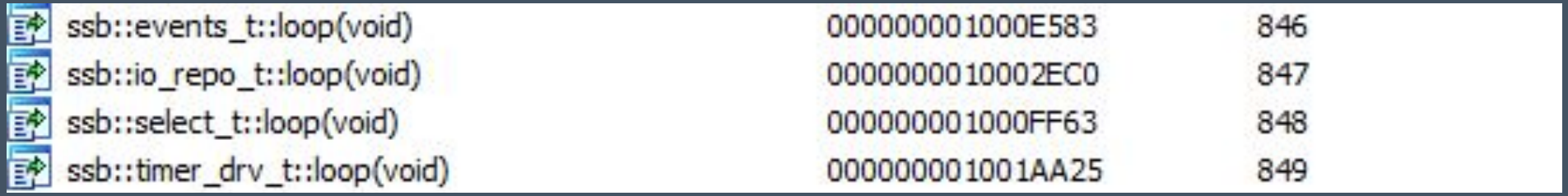
Critical Zoom Vulnerability CVE-2018-15715




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

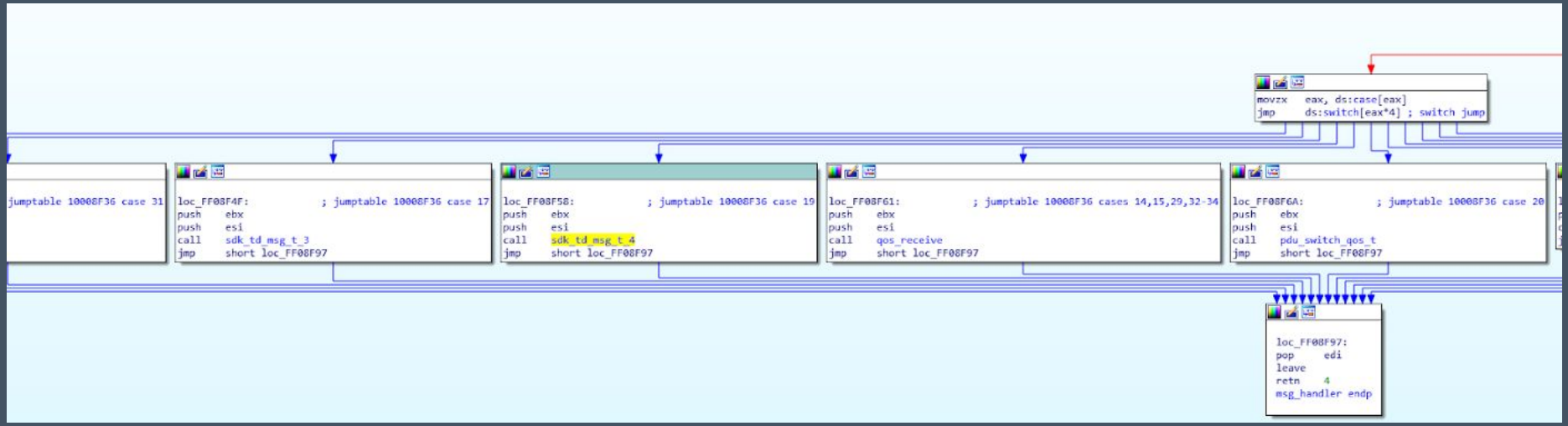

tenable

Critical Zoom Vulnerability CVE-2018-15715



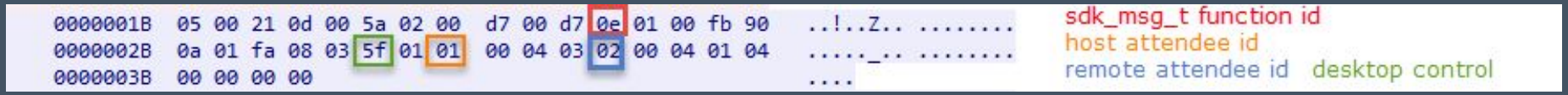
tenable

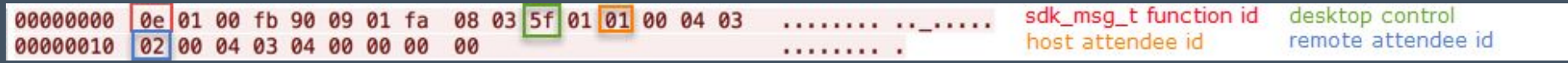
Critical Zoom Vulnerability CVE-2018-15715



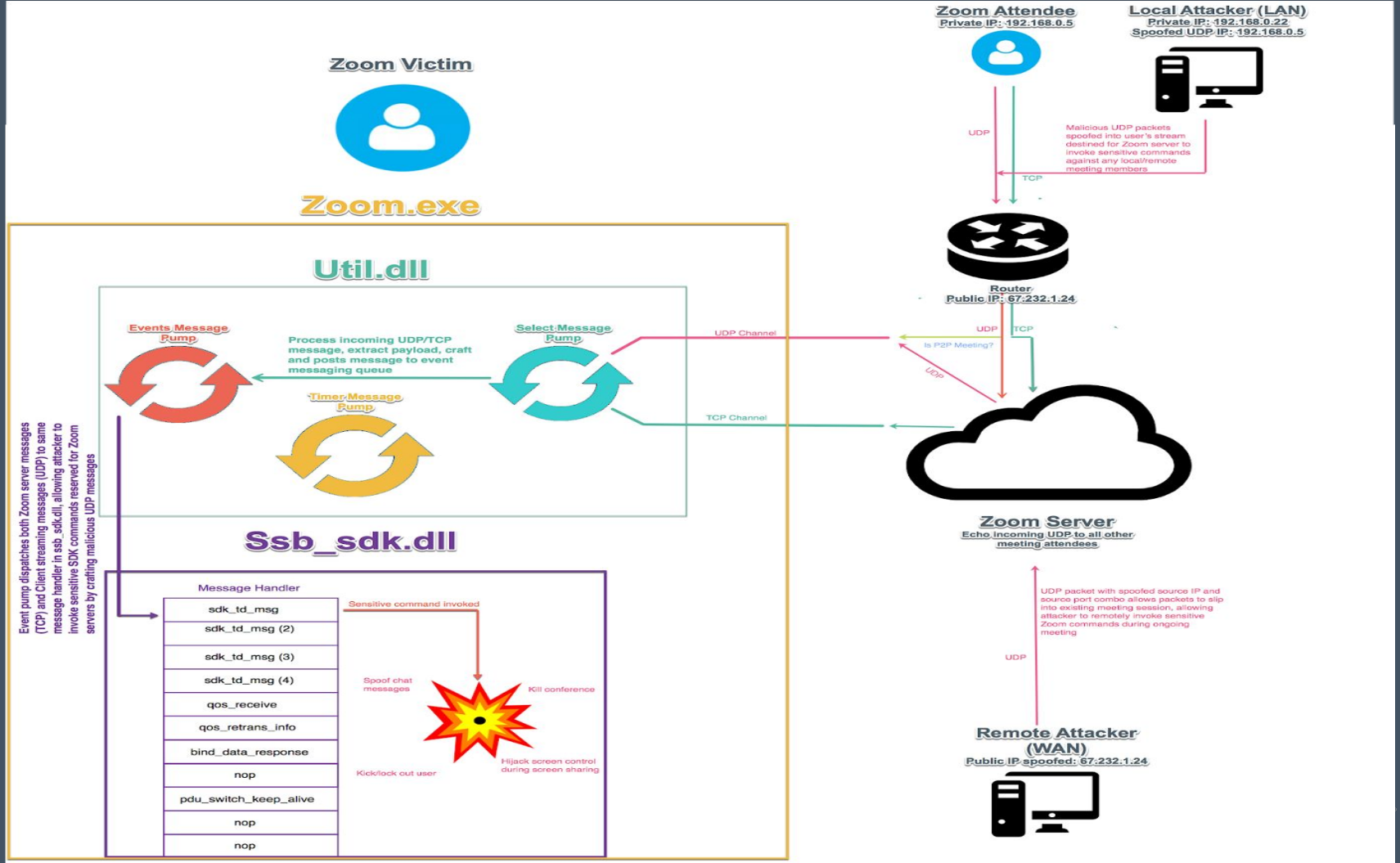
tenable

Critical Zoom Vulnerability CVE-2018-15715





tenable


Zoom Victim
Zoom.exe
Util.dll
Events Message Pump
Process incoming UDP/TCP message, extract payload, craft and posts message to event messaging queue
Select Message Pump
Timer Message Pump
Event pump dispatches both Zoom server messages (TCP) and Client streaming messages (UDP) to same message handler in ssb_sdk.dll, allowing attacker to invoke sensitive SDK commands reserved for Zoom servers by crafting malicious UDP messages
Ssb_sdk.dll
Message Handler
sdk_td_msg
sdk_td_msg (2)
sdk_td_msg (3)
sdk_td_msg (4)
qos_receive
qos_retrans_info
bind_data_response
nop
pdu_switch_keep_alive
nop
nop
Sensitive command invoked
Spoof chat messages
Kill conference
Kick/lock out user
Hijack screen control during screen sharing
UDP Channel
TCP Channel
Zoom Attendee
Private IP: 192.168.0.5
Local Attacker (LAN)
Private IP: 192.168.0.22
Spoofed UDP IP: 192.168.0.5
UDP
TCP
Malicious UDP packets spoofed into user's stream destined for Zoom server to invoke sensitive commands against any local/remote meeting members
Router
Public IP: 67.232.1.24
Is P2P Meeting?
Zoom Server
Echo incoming UDP to all other meeting attendees
UDP packet with spoofed source IP and source port combo allows packets to slip into existing meeting session, allowing attacker to remotely invoke sensitive Zoom commands during ongoing meeting
Remote Attacker (WAN)
Public IP spoofed: 67.232.1.24

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/xmppconnection.lua

Port 8088
    ** WebSocket **
       Used for local network SmartPhone App connectivity and commanding
    -> Web socket request
       {"hbus":{"id":"xyxxxyxxxxxxxxx#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/smartthings.lua
          http://<ipAddress>:8222/api/harmony.automation?smartthingscb
```

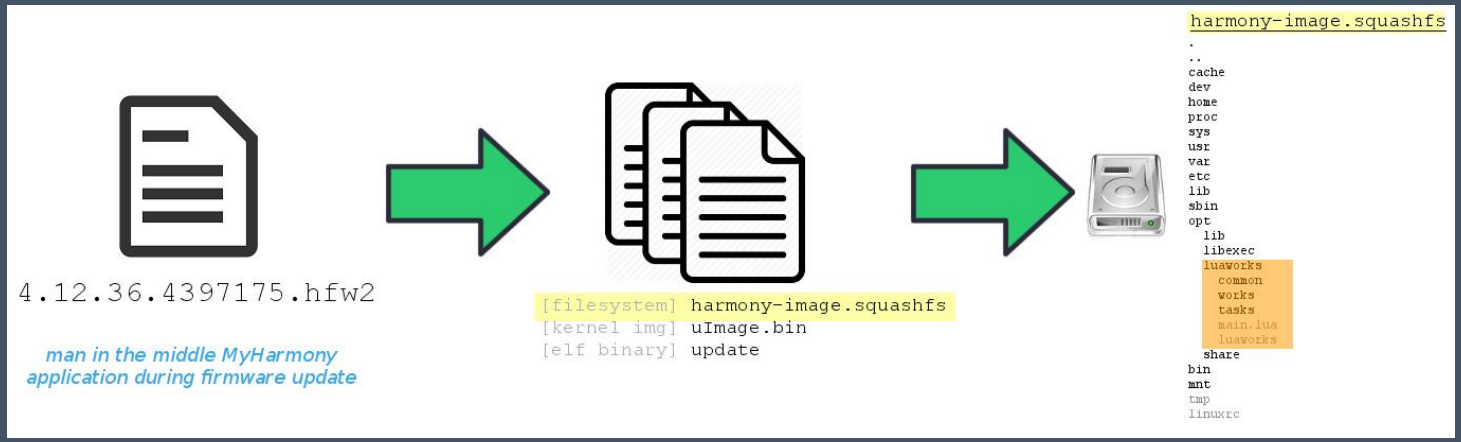
tenable

Device
Firmware

Firmware - MyHarmony app

- Lua 5.1 application code

  using OpenWRT patches *(important for decompilation)*



tenable

Device

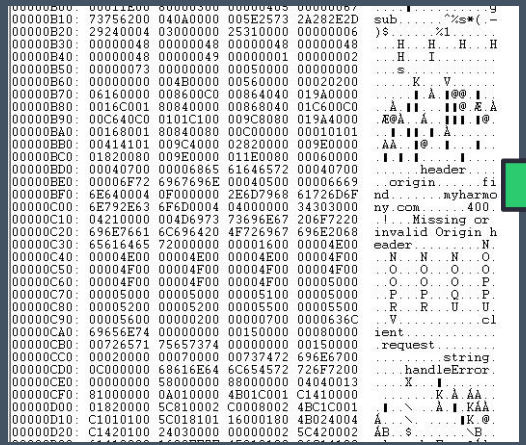
Application Code

OpenWRT Lua interpreter patches

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

Lua decompilation

https://github.com/viruscamp/luadec



```
00000B10: 73756200 040A0000 005E2573 2A282E2D  sub.....^%s*(.-
00000B20: 29240004 03000000 25310000 00000006  )$......%1......
00000B30: 00000048 00000048 00000048 00000048  ...H...H...H...H
00000B40: 00000048 00000049 00000001 00000002  ...H...I........
00000B50: 00000073 00000000 00050000 00000000  ...s............
00000B60: 00000000 004B0000 00560000 00020200  .....K...V......
00000B70: 06160000 008600C0 00864040 019A0000  ........@@......
00000B80: 0016C001 80840000 00868040 01C600C0  ..À.....@.Æ.À
00000B90: 00C640C0 0101C100 009C8080 019A4000  .Æ@À..Á.....@.
00000BA0: 00168001 80840080 00C00000 00010101  ..........À.....
00000BB0: 00414101 009C4000 02820000 009E0000  .AA...@.........
00000BC0: 01820080 009E0000 011E0080 00060000  ................
00000BD0: 00040700 00006865 61646572 00040700  ......header....
00000BE0: 00006F72 6967696E 00040500 00006669  ..origin......fi
00000BF0: 6E640004 0F000000 2E6D7968 61726D6F  nd.......myharmo
00000C00: 6E792E63 6F6D0004 04000000 34303000  ny.com.....400..
00000C10: 04210000 004D6973 73696E67 206F7220  .!...Missing or
00000C20: 696E7661 6C696420 4F726967 696E2068  invalid Origin h
00000C30: 65616465 72000000 00001600 00004E00  eader.........N.
00000C40: 00004E00 00004E00 00004E00 00004F00  ..N...N...N...O.
00000C50: 00004F00 00004F00 00004F00 00004F00  ..O...O...O...O.
00000C60: 00004F00 00004F00 00004F00 00005000  ..O...O...O...P.
00000C70: 00005000 00005000 00005100 00005000  ..P...P...Q...P.
00000C80: 00005200 00005200 00005500 00005500  ..R...R...U...U.
00000C90: 00005600 00000200 00000700 0000636C  ..V...........cl
00000CA0: 69656E74 00000000 00150000 00080000  ient............
00000CB0: 00726571 75657374 00000000 00150000  .request........
00000CC0: 00020000 00070000 00737472 696E6700  .........string.
00000CD0: 0C000000 68616E64 6C654572 726F7200  ....handleError.
00000CE0: 00000000 58000000 88000000 04040013  ....X...........
00000CF0: 81000000 0A010000 4B01C001 C1410000  ........K.À.ÁA..
00000D00: 01820000 5C810002 C0008002 4BC1C001  ....\...À...KÁÀ.
00000D10: C1010100 5C018101 16000180 4B024004  Á...\.....K.@.
00000D20: C1420100 24030000 00000002 5C42D002  ÁB..$.......\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      return false
64    end
65    return true
66  end
```

tenable

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

tenable

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

tenable

Vulns

remote server os command injection

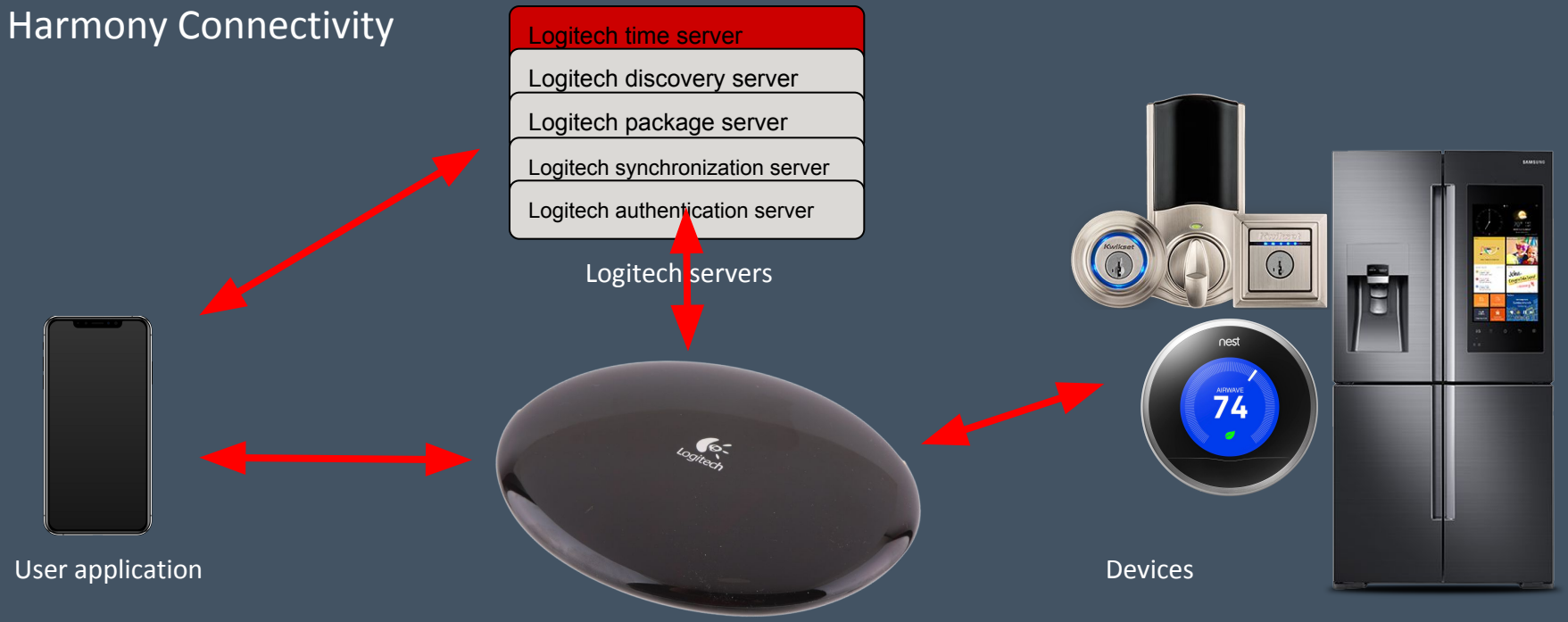
Harmony Connectivity

tenable

Vulns

remote server os command injection

Harmony Connectivity



tenable

Vulns

remote server os command injection

Patch Diff

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
140
141
142       local clocksetStr = "date -s \"" .. time.utc .. "\""
143       local before = (os.time)()
144       ;
145       (os.execute)(clocksetStr)
146       ;
147       (system.tiggleWatchDog)("time is changed from " .. before .. " to " .. (os.
```

Patched

```
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*:%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.tiggleWatchDog)("time is changed from " .. before .. " to " .. (os.
```

tenable

Vulns

application command execution

Vulnerability

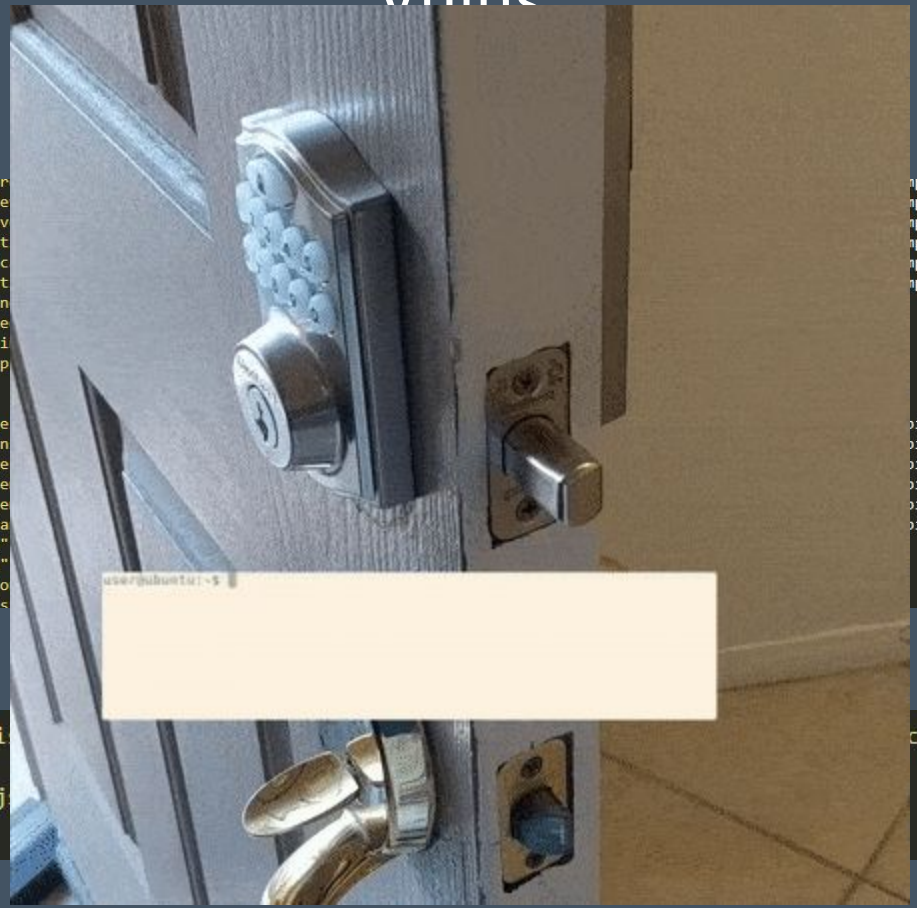
```
local handlePost = function(client, clientId, request, hbusMsg)
  (clientConnections.addClientConnection)(clientId, "hbushttp", client)
  if not (request.header)["content-type"] or not (string.match)((request.header)["content-type"], "application/json") then
    return handleError(client, clientId, "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
```

tenable

Vulns



Exploit

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

tenable

Questions, comments, concerns?

Please reach out!

@dinobytes @lynerc

@CE2Wells @pneumagennao

tenable