Analyzing Raw Binary Images in Ghidra

A Look at Cisco IOS

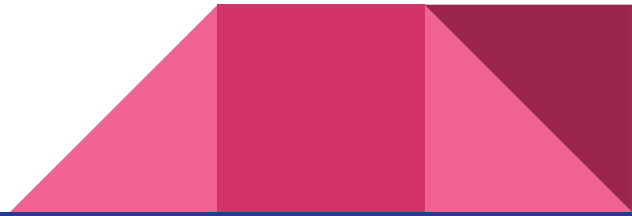
Who am I?

Nick Starke - Security Researcher located in Des Moines.

Works for Aruba Networks/HPE as a Threat Researcher / Reverse Engineer

Likes building and breaking

Bugcrowd MVP



What is Ghidra?

Reverse Engineer / Binary Analysis Platform built by NSA Research Directorate

Released in early 2019

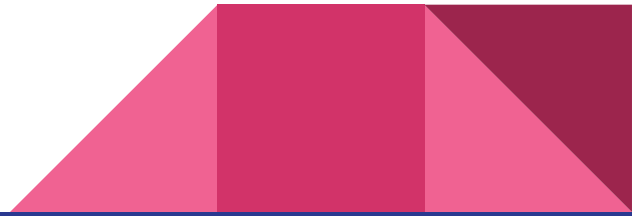
Competitor (in some ways) to IDA Pro, Binary Ninja, and Radare2

The Story so far...

In Mid 2018 I bought a Cisco Catalyst 3750 off eBay.

I was gonna hack a switch.

I had no idea what I was doing.

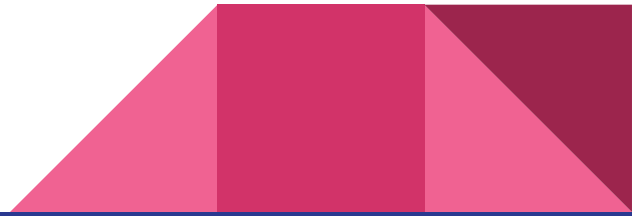


Firmware File Layout

First 112 (0x70) Bytes are a proprietary header

Firmware image begins as index 112.

How did I figure that out?



Binwalk

https://github.com/refirmlabs/binwalk

Run

$ binwalk -eM firmware_file.bin

-e for auto extract

-M for recursive

Bzip2 Data at 0x70

```
┌──(~/Documents/research/cisco-catalyst-3750)
└─➤ binwalk c3750-ipservicesk9-mz.122-50.SE3.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
112           0x70            bzip2 compressed data, block size = 900k
```

Now that we have the bunzipped image...

We need to figure out what CPU architecture the image is built for:

```
└──➤ binwalk -m /usr/local/lib/python2.7/dist-packages/binwalk/magic/binarch _c3750-ipservicesk9-mz.122-50.SE3.0002.bin.extracted/70

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
24            0x18            PowerPC big endian instructions, function prologue
1360          0x550           PowerPC big endian instructions, function epilogue
1364          0x554           PowerPC big endian instructions, function epilogue
1372          0x55C           PowerPC big endian instructions, function epilogue
1380          0x564           PowerPC big endian instructions, function epilogue
1388          0x56C           PowerPC big endian instructions, function prologue
1612          0x64C           PowerPC big endian instructions, function epilogue
1648          0x670           PowerPC big endian instructions, function epilogue
1656          0x678           PowerPC big endian instructions, function prologue
3224          0xC98           PowerPC big endian instructions, function epilogue
3232          0xCA0           PowerPC big endian instructions, function prologue
6772          0x1A74          PowerPC big endian instructions, function epilogue
6780          0x1A7C          PowerPC big endian instructions, function prologue
```

Binwalk magic mode

Binwalk’s magic numbers can be reconfigured.

Binwalk comes with a magic definition file called “binarch”

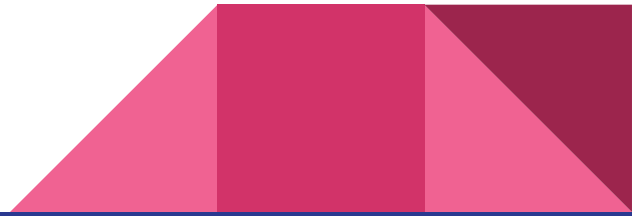
We use this file with the “-m” flag to produce the aforementioned output

Clearly, it is likely this is a Big Endian PowerPC firmware image.

Finding Offset values

A Switch OS does not start at memory address 0x00000000

We must go deeper...

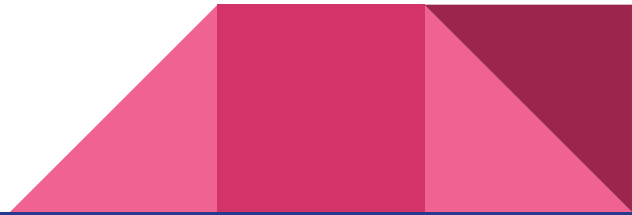


Show version

From the serial or ssh console, we run `show version`

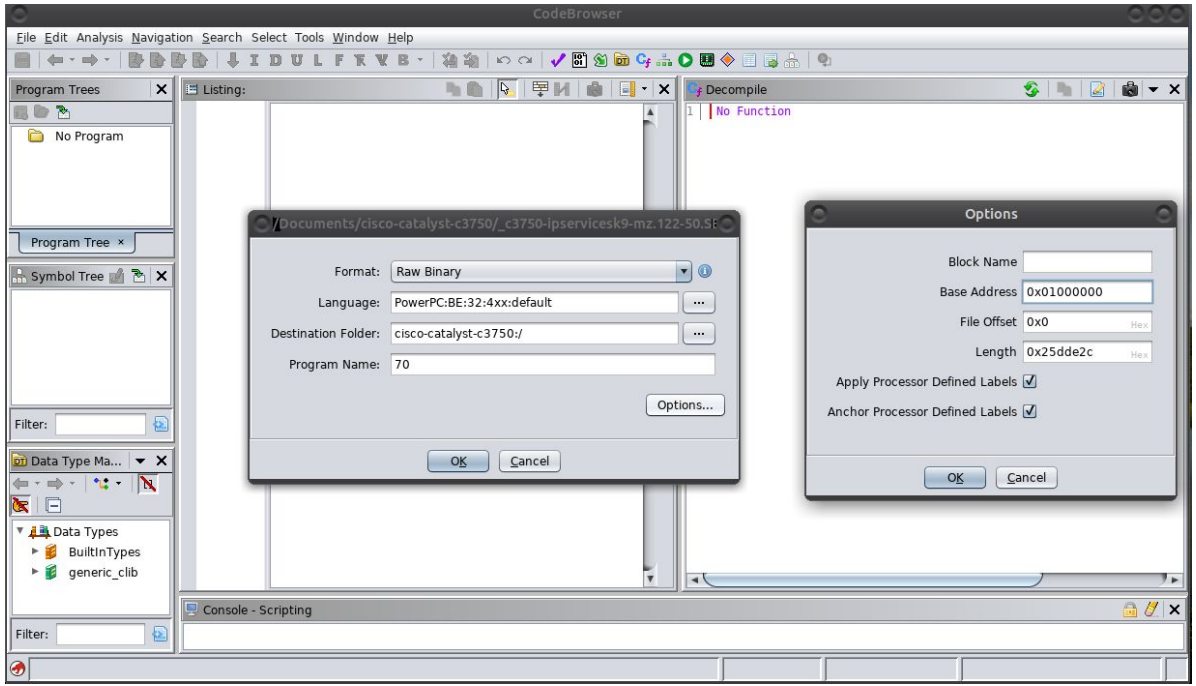
That gives us an OS load address of 0x01000000

```
Switchy>show version
Cisco IOS Software, C3750 Software (C3750-IPSERVICESK9-M), Version 12.2(55)SE, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc.
Compiled Sat 07-Aug-10 22:45 by prod_rel_team
Image text-base: 0x01000000, data-base: 0x02F00000
```

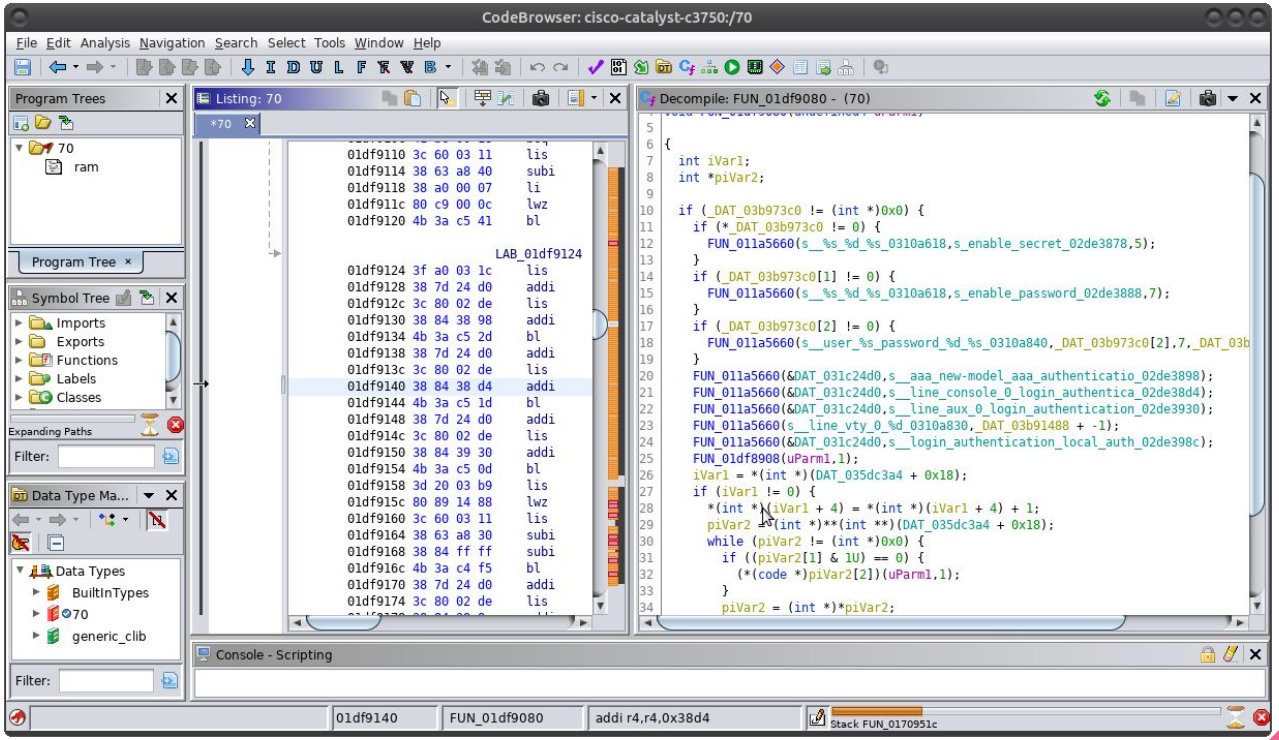


Time to Fire up Ghidra!

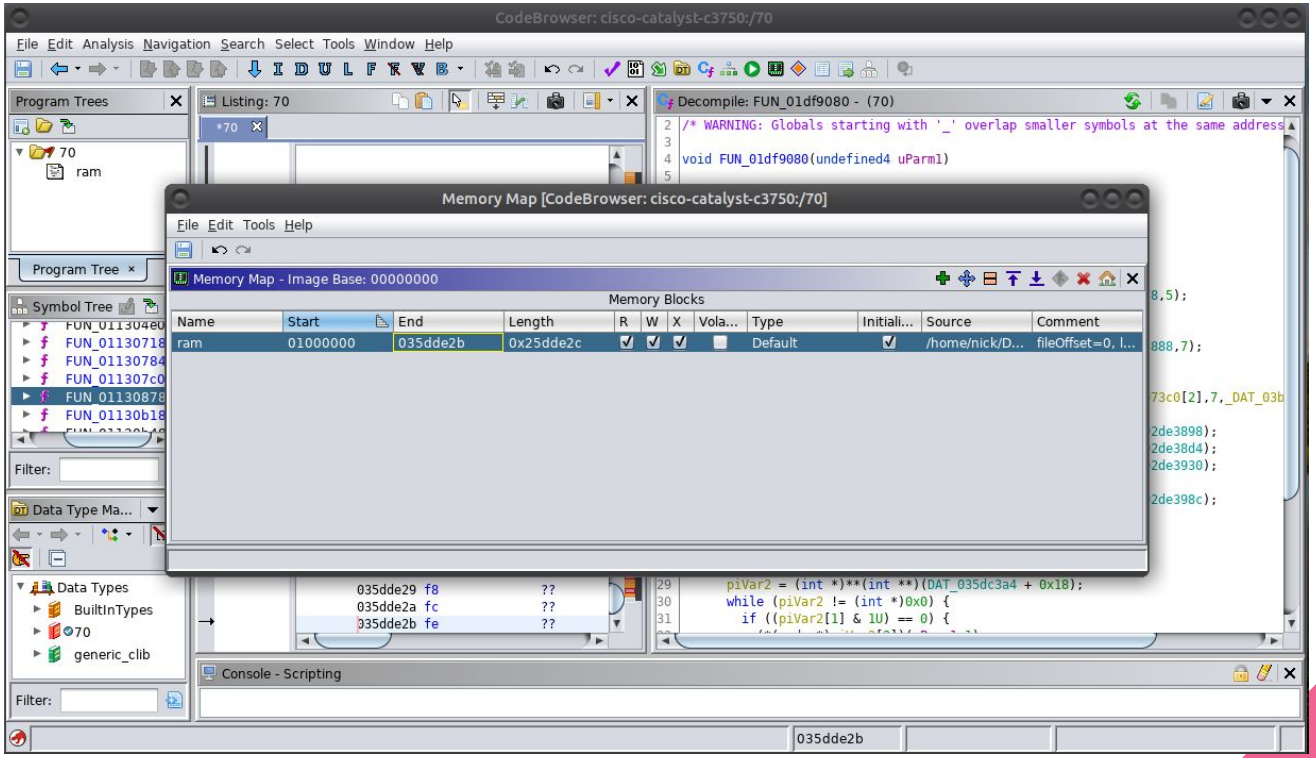
We need to load our bunzipped firmware image into Ghidra:



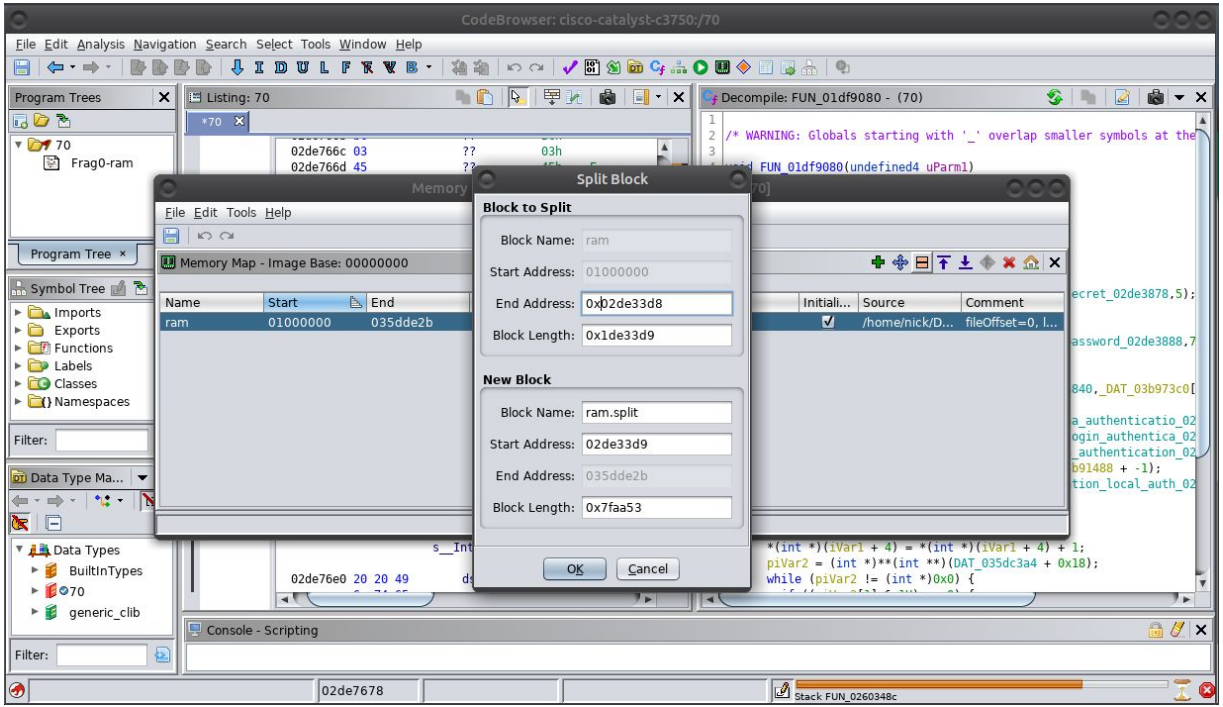
Ghidra will Churn



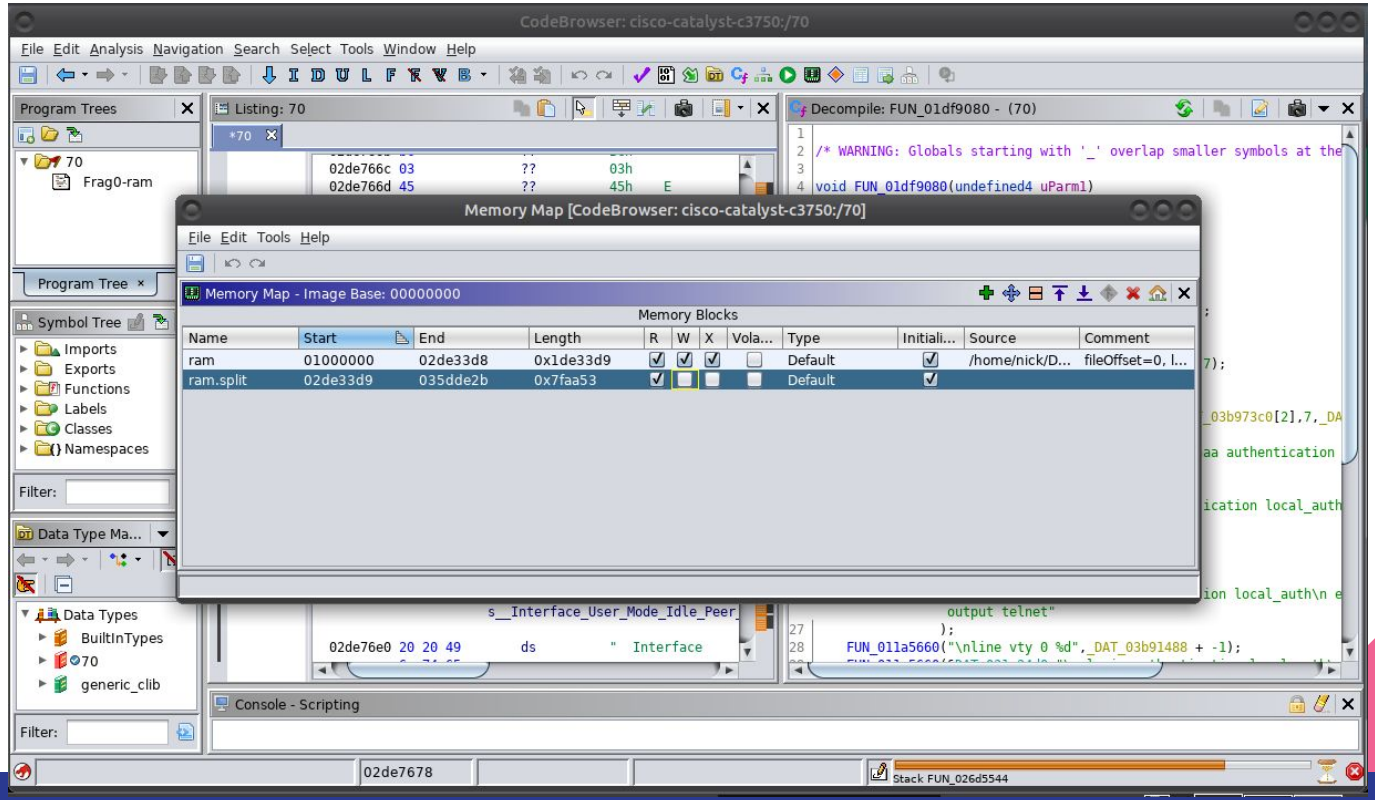
Setting the Data-base



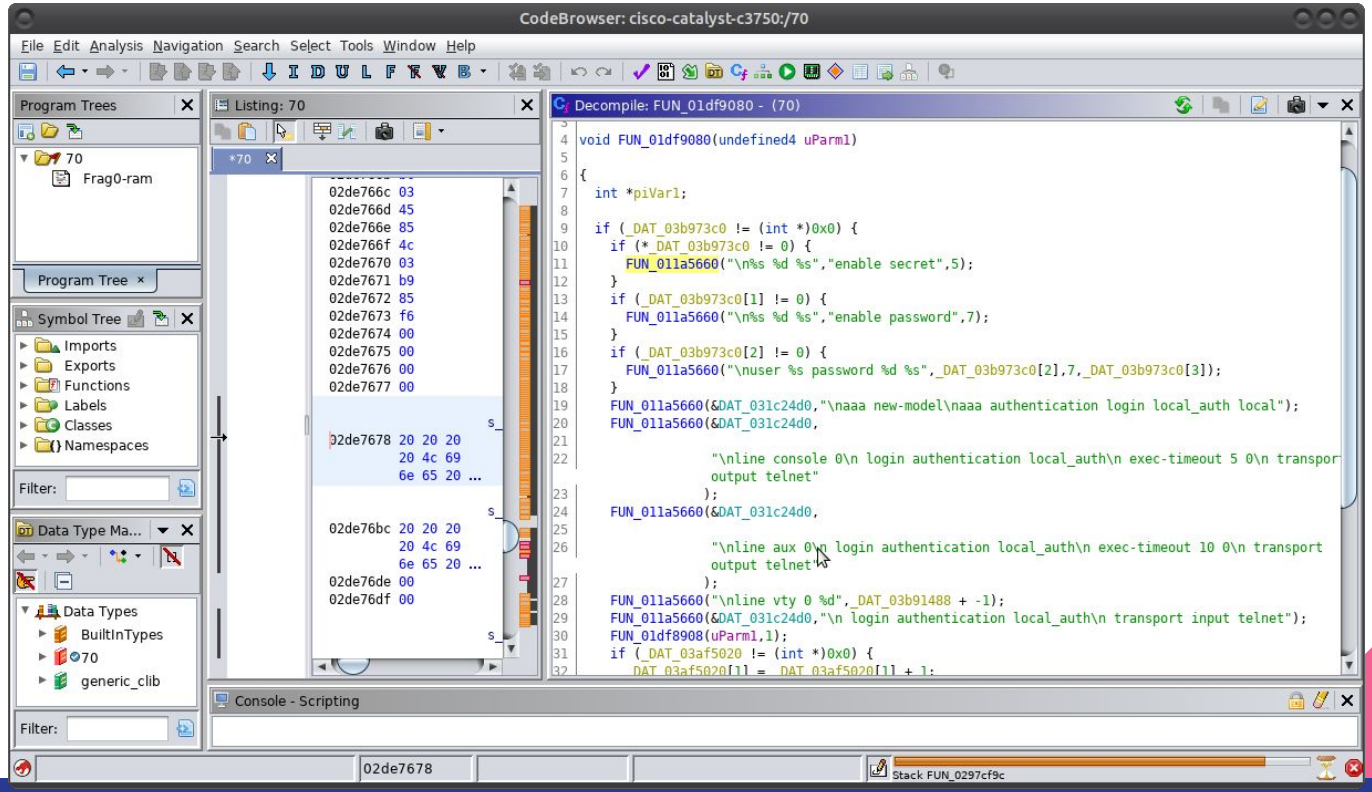
Splitting Memory



Splitting Memory Continued (RWX)



Resolved Strings



Live Demo

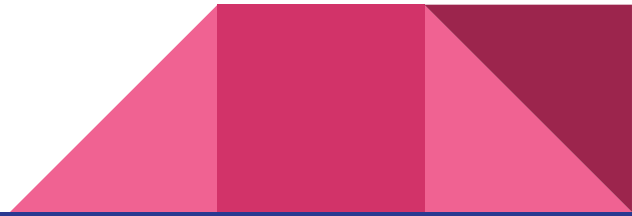
“CISCO KITS”

https://artkond.com/2017/04/10/cisco-catalyst-remote-code-execution

Linky

This whole presentation is based on a write up I did:

https://gist.github.com/nstarke/ed0aba2c882b8b3078747a567ee00520



Questions?

Thank you!

Contact:

@nstarke on secdsm slack

@nstarke on twitter

@nstarke on github