

# DSLAMing

TESTING WAN SERVICES ON DSL MODEMS

# New Presentation, Who dis?

Nick Starke

- Security Researcher at Aruba Threat Labs (Aruba Networks' internal Red Team)
- Local to Des Moines, IA area
- Member of SecDSM and Iowa ISSA
- IoT device / Networking Equipment enthusiast extraordinaire

# What is a DSLAM? Some definitions real quick

## **Digital Subscriber Line Access Multiplexer (DSLAM)**

The headend unit for DSL Modems.

Communicates via ATM (more on this later).

## **Digital Subscriber Line (DSL) Modem**

The **Customer Premises Equipment (CPE)** that attaches downstream from a DSLAM

# Disclaimer!!!!

I have never worked for an ISP.

I have never configured a DSLAM for a production environment.

I have only used DSLAMs in tightly controlled network security lab environments.

This talk is not about configuring a DSLAM securely!

# Ok great so what is this talk actually about then?

This presentation is about using a DSLAM to test **Wide Area Network (WAN)** services on DSL modems.

We'll cover:

- Network fingerprint of a DSLAM
- Physical configuration of lab environment
- Basic configuration gotchas for both DSLAM and lab DSL modem
- How to source a DSLAM

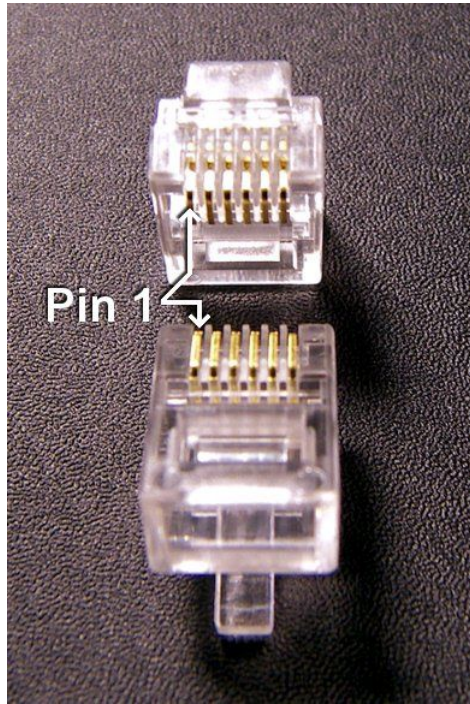
And most importantly:

- Why would anyone want to do this?

# DSL Modems as IoT Devices

- Non-ethernet WAN port
- Ethernet uses RJ-45
- DSL Modems / Traditional Phone Systems use RJ-14
- Most DSL Modems have a variety of network services running on them
- Attack Surface is generally large because of network services

# RJ-14 vs RJ-45 (6-pin versus 8-pin)



# RJ-21 (WAN Connection Cable)

Male





# RJ-21 (WAN Connection Cable)



# RJ-21 (WAN Connection Cable)

Female RJ-21 (the bright blue):

Pictured: Two DSLAMs



# ZyXEL IES-1000



# ZyXEL IES-1000

1U Form Factor

Two slots for network interface cards

RJ-21 and RJ-14 cards available

Price on Ebay: \$150-\$250 (occasionally cheaper!)

# VersaTek - VX1000LD



# VersaTek VX1000LD

1U Form factor

Comes with RJ-21 port and ethernet uplink

No interchangeable card slots

Price: \$75-\$150

Note that RJ21 cables run from \$75-\$100 and you will have to have one to connect downstream devices

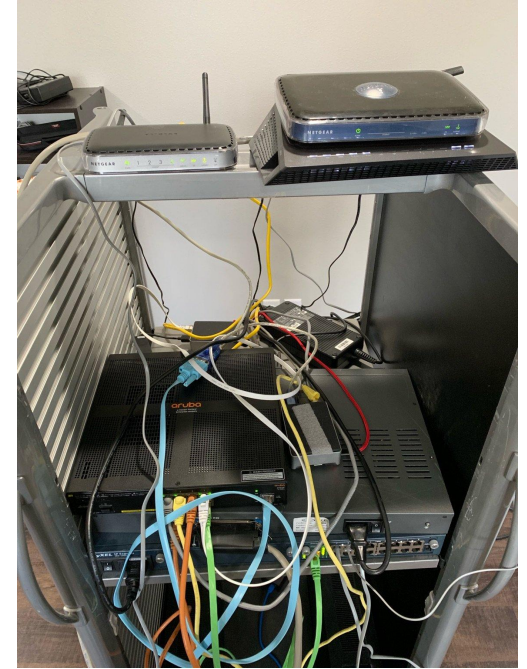
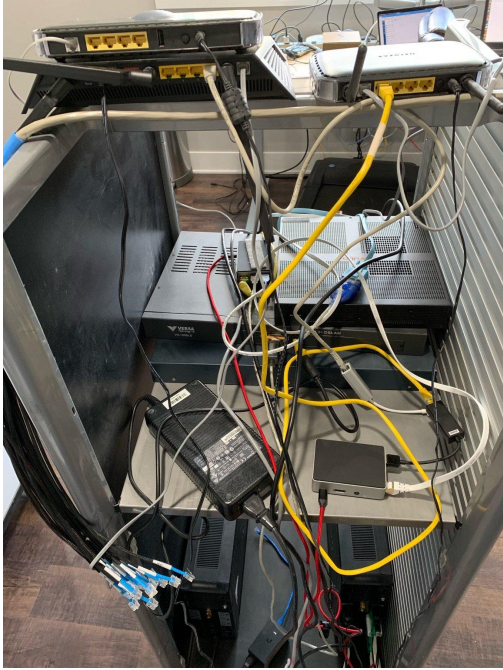
# WARNING

The following slide includes graphic depictions of cabling.

**Viewer Discretion is Advised.**



# Lab build out for this presentation





# Lab build out for this presentation (Inventory)

- Aruba 2930f - Core switch
- Zyxel IES 1000 - DSLAM
- Two Raspberry Pis
  - One on the WAN side
  - The other has two NICs, one on the WAN side for remote access, and one on the LAN side of a DSL Modem
- Three DSL Modems
  - Netgear DGN2000
  - Netgear D7000
  - ActionTec C1000a - CenturyLink Branded

## Cool, where can I buy one?

The best place to source DSLAMs cheaply is eBay.

Depending on what kind you want, prices run from about \$150-\$1000

You can get a good DSLAM for \$150 (check out ZyXEL IES-1000)

Sometimes Amazon carries second hand DSLAMs, but the price is often inflated.

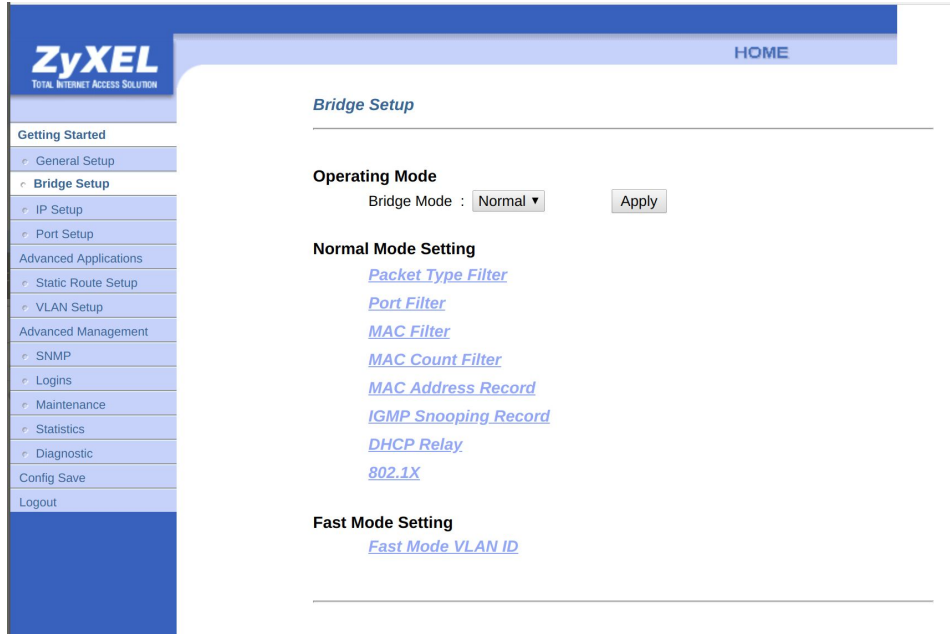
# Basic Configuration

DHCP is very important. Most DSL modems will not accept a WAN DHCP lease without defined values for DHCP options:

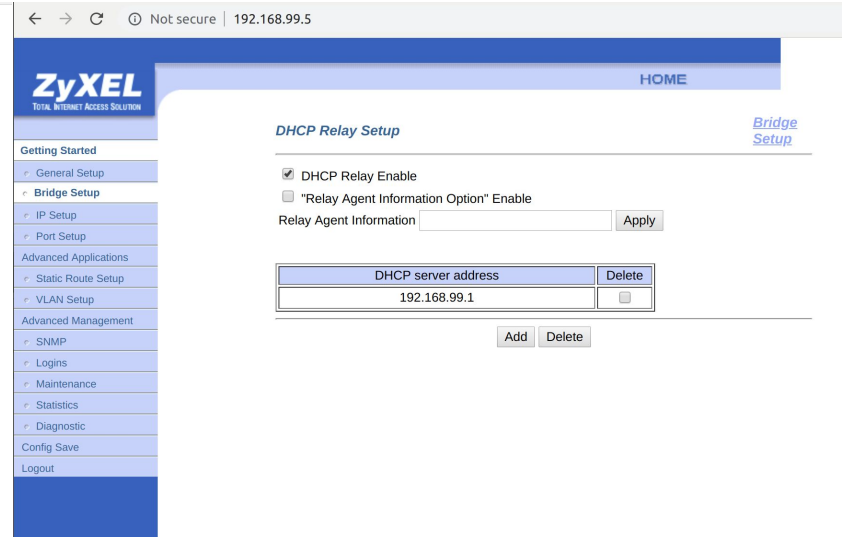
- DNS Server Address
- Gateway address

DHCP Relay is also important, if your DSLAM offers it (IES-1000 does):

# IES-1000 DHCP Relay via Web Interface



The screenshot shows the ZyXEL web interface for the Bridge Setup page. The left sidebar contains a navigation menu with the following items: Getting Started (General Setup, Bridge Setup, IP Setup, Port Setup), Advanced Applications (Static Route Setup, VLAN Setup), Advanced Management (SNMP, Logins, Maintenance, Statistics, Diagnostic), Config Save, and Logout. The main content area is titled "Bridge Setup" and includes a "HOME" link. Under "Operating Mode", the "Bridge Mode" is set to "Normal" with an "Apply" button. Below this, there are two sections: "Normal Mode Setting" with links for Packet Type Filter, Port Filter, MAC Filter, MAC Count Filter, MAC Address Record, IGMP Snooping Record, DHCP Relay, and 802.1X; and "Fast Mode Setting" with a link for Fast Mode VLAN ID.



The screenshot shows the ZyXEL web interface for the DHCP Relay Setup page. The left sidebar is identical to the previous screenshot. The main content area is titled "DHCP Relay Setup" and includes a "HOME" link and a "Bridge Setup" link. Under "Getting Started", the "DHCP Relay Enable" checkbox is checked, and the "Relay Agent Information Option" checkbox is unchecked. There is an "Apply" button next to the "Relay Agent Information" field. Below this, there is a table for DHCP server addresses:

DHCP server address	Delete
192.168.99.1	<input type="checkbox"/>

At the bottom of the table, there are "Add" and "Delete" buttons.

# IES-1000 Network Fingerprint

```
Host is up (0.0015s latency).
Not shown: 65477 closed ports, 55 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
80/tcp    open  http
MAC Address: 00:13:49:7C:EB:5D (ZyXEL Communications)

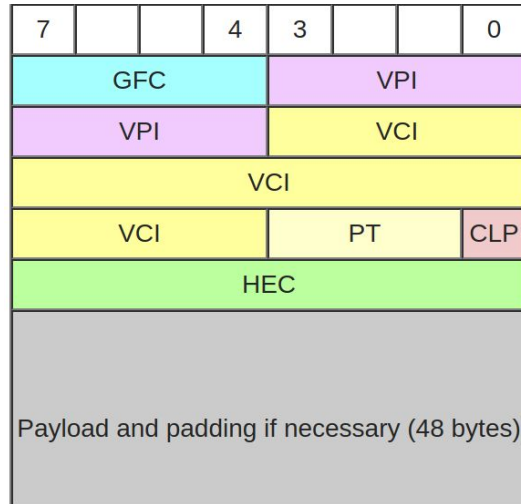
Host is up (0.0014s latency).
Not shown: 996 closed ports
PORT      STATE      SERVICE
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
161/udp   open|filtered snmp
520/udp   open|filtered route
MAC Address: 00:13:49:7C:EB:5D (ZyXEL Communications)
```

# Operating System?

Most DSLAMs run a vendor-specific proprietary **Real Time Operating System (RTOS)** that is not publicly available, let alone open source.

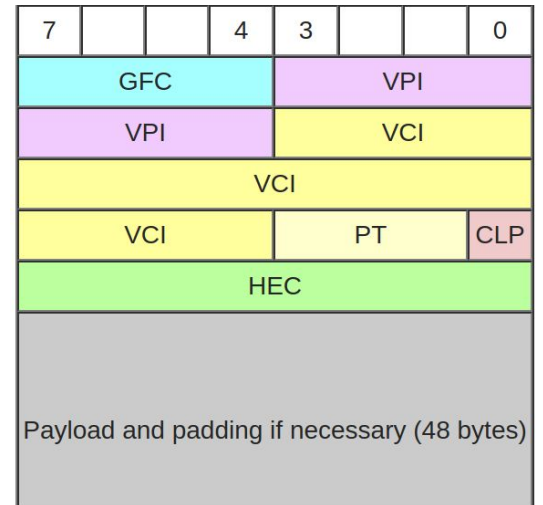
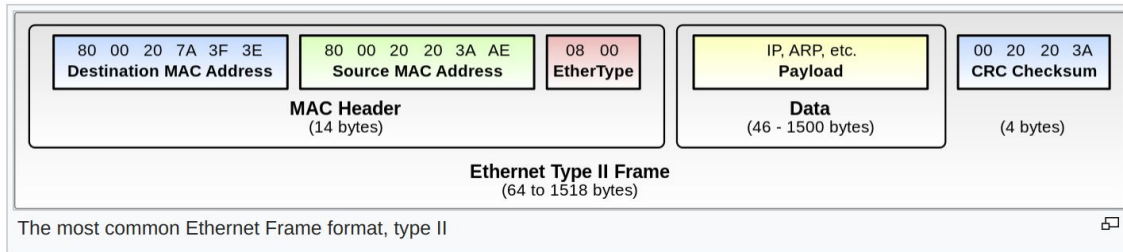
# DSLAM Protocols

The Layer 2 protocol used in communication between the DSLAM and the DSL Modem WAN port is **Asynchronous Transfer Mode (ATM)**.



*Source: wikipedia.org*

# ATM Versus Ethernet



Source: *wikipedia.org*



## ATM Versus Ethernet (Continued)

ATM is divided into **cells**, each of which has a 5 byte header and 48 byte payload for a total of 53 bytes per cell.

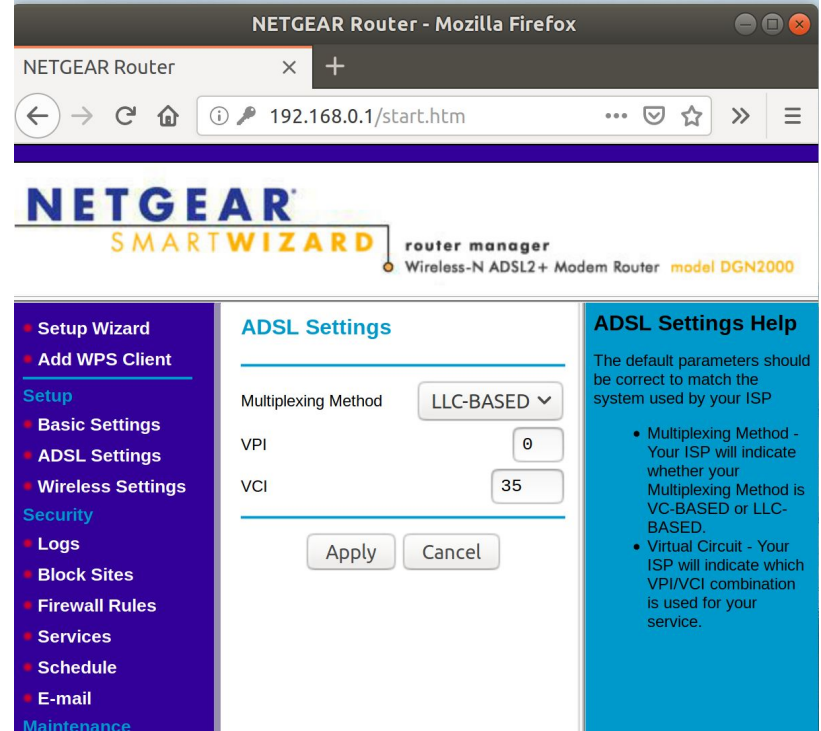
Ethernet is divided into **frames**, of which the **data** section is variable length.

# VPI and VCI turn out to be important

**VCI = Virtual Circuit Identifier**

**VPI = Virtual Path Identifier**

Whatever is configured on DSLAM must equal whatever is configured on the DSL Modem.



# VPI and VPC Uses

- **Quality of Service (QoS)**
- Traffic Shaping
- Traffic Policing

# So now that we have built this huge lab...

Why does anyone care about this?

- DSL Modems can have network services running on the WAN port

Let's say you're writing an exploit that is delivered via **Cross-Site Request Forgery (CSRF)**, and the exploit is designed to start a telnet daemon on the WAN interface. There's no other way to test such capabilities.

- Many times DSL Modems have secondary firewalls built in to protect the WAN port, making tools like **netstat** insufficient (if it is even on the filesystem).

## So for testing exploits? Is that all?

Additionally, DSL modems (like any other sort of network device) often establish connections to manufacturer hosts to check for updates or receive support.

Again, the only way to test / capture such traffic is to use a DSLAM and then perhaps a mirror port on your **Core Switch**.

You will not be able to capture level 2 (ATM) traffic, but you will see reconstructed ethernet packets with the application level packet data intact.

# Ok so exploit dev and traffic analysis...

Every once in a while you'll find a manufacturer backdoor:

<https://github.com/elvanderb/TCP-32764>

Backdoor found in Sercomm products in 2014.

# Exploit Development

Sometimes DSL Modems have WAN services that are exploitable, but most of the time the WAN is firewalled so that all 65535 ports are filtered.

In this case, it becomes necessary to “convince” the user (behind the firewall) to perform some action that exploits a LAN-based vulnerability which either returns a reverse shell, or opens a port on the WAN.

If the vulnerability is in the Web interface, CSRF works well for delivering Command Injection exploits because very few DSL Modems have Anti-CSRF protections.

# Traffic Analysis

Certain DSL Modems will auto update by fetching a newer firmware version from a manufacturer host.

Sometimes the firmware update comes in the form of an executable shell script with embedded binary.

Sometimes the download happens over HTTP/FTP without any sort of encryption.



## Traffic Analysis (continued)

The best way to capture WAN traffic from DSL Modems is to use a mirror port on the upstream switch. If you work one DSL modem at a time, there won't be an overwhelming amount of traffic.

# Backdoor

The **TCP-32764** backdoor was discovered in 2014, affecting most if not all Sercomm products.

This was an open port (32764) which returned anyone accessing it a root shell

While mostly this affected the LAN-side of devices, there were some that also had this problem on the WAN port.

# Taking a step back

So we've now seen why someone might want to test DSL modem WAN interfaces using a DSLAM.

But let's take a step back and ask a bigger question:

**“Why would anyone want to hack a DSL Modem?”**

# Exploit Scenarios

The first exploit scenario is the most common with DSL modems / **Small Office Home Office (SoHo)** network equipment:

- 1) Change the upstream DNS server configuration to point to an attacker controlled DNS server
- 2) Redirect all DNS traffic to attacker controlled infrastructure
- 3) Steal credentials as they come over the wire

# Man in the Middle Scenarios

Since a DSL modem acts as a network gateway, all traffic on the network flows through it. Having this sort of vantage point as an attacker makes mounting **Man in the Middle (MitM)** attacks trivial (as long as you can compile TCPDUMP for the target architecture). An attacker can sniff / modify traffic as it goes over the wire, exposing plaintext credentials as well as other sensitive data.

# Pivot Scenarios

Along the lines of the MitM attack, an attacker can use this position on a network to pivot to other devices behind the DSL Modems' WAN firewall. Since most DSL Modems run everything as root, once you have a working exploit, you have root access to the DSL Modem.

This allows an attacker to mount further attacks against endpoints on the LAN.

# Botnet Scenarios

Find a vulnerability, exploit it to add the DSL Modem to a botnet.

This utilizes the traffic / bandwidth of the DSL modem to overwhelm a specific target in concert with other compromised IoT devices.

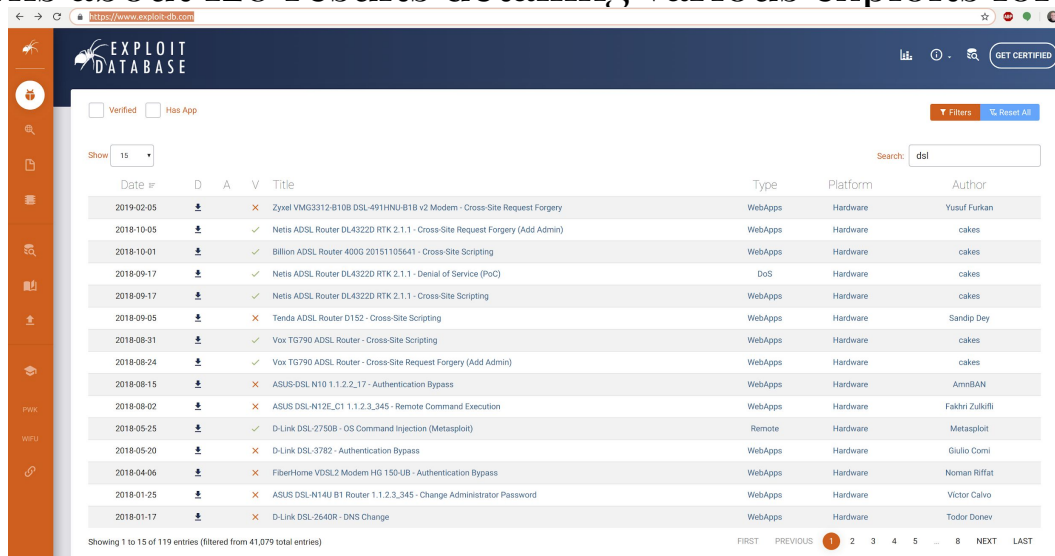
The Mirai botnet is the best example of this type of behavior.

# Where can I find more information on DSL Modem Exploits?

<https://www.exploit-db.com/>

Search for DSL.

Currently returns about 120 results detailing various exploits for DSL Modems.



The screenshot shows the Exploit Database search results for the query 'dsl'. The interface includes a search bar with the query 'dsl' and a 'Filters' button. The results are displayed in a table with columns for Date, Verified status, Author, Title, Type, and Platform. The table shows 15 results, with a 'Showing 1 to 15 of 119 entries' indicator at the bottom. The results include various exploits for different DSL modems, such as Zyxel VMG3312-810B, Netis ADSL Router DL4322D, and ASUS DSL-N14J B1.

Date	Verified	Author	Title	Type	Platform
2019-02-05	✗	Yusuf Furkan	Zyxel VMG3312-810B DSL-491HNU-B18 v2 Modem - Cross-Site Request Forgery	WebApps	Hardware
2018-10-05	✓	cakes	Netis ADSL Router DL4322D RTK 2.1.1 - Cross-Site Request Forgery (Add Admin)	WebApps	Hardware
2018-10-01	✓	cakes	Billion ADSL Router 4000 20151105641 - Cross-Site Scripting	WebApps	Hardware
2018-09-17	✓	cakes	Netis ADSL Router DL4322D RTK 2.1.1 - Denial of Service (PoC)	DoS	Hardware
2018-09-17	✓	cakes	Netis ADSL Router DL4322D RTK 2.1.1 - Cross-Site Scripting	WebApps	Hardware
2018-09-05	✗	Sandip Dey	Tenda ADSL Router D152 - Cross-Site Scripting	WebApps	Hardware
2018-08-31	✓	cakes	Vox TG790 ADSL Router - Cross-Site Scripting	WebApps	Hardware
2018-08-24	✓	cakes	Vox TG790 ADSL Router - Cross-Site Request Forgery (Add Admin)	WebApps	Hardware
2018-08-15	✗	ArneBAN	ASUS-DSL-N10 1.1.2.2.17 - Authentication Bypass	WebApps	Hardware
2018-08-02	✗	Fakri Zukuffi	ASUS DSL-N12E_C1 1.1.2.3.345 - Remote Command Execution	WebApps	Hardware
2018-05-25	✓	Metasploit	D-Link DSL-2750B - OS Command Injection (Metasploit)	Remote	Hardware
2018-05-20	✗	Giulio Corni	D-Link DSL-3782 - Authentication Bypass	WebApps	Hardware
2018-04-06	✓	Noman Rifat	FiberHome VDSL2 Modem HG 150-UB - Authentication Bypass	WebApps	Hardware
2018-01-25	✗	Victor Calvo	ASUS DSL-N14J B1 Router 1.1.2.3.345 - Change Administrator Password	WebApps	Hardware
2018-01-17	✗	Todor Donev	D-Link DSL-2640R - DNS Change	WebApps	Hardware



# Examples

- <https://www.quantumleap.it/d-link-router-dsl-2750b-firmware-1-01-1-03-rce-no-auth/>
- [https://www.vulnerability-lab.com/get\\_content.php?id=1591](https://www.vulnerability-lab.com/get_content.php?id=1591)
- <https://www.exploit-db.com/exploits/45532>

## In Summary

A DSLAM can be a useful tool for developing and testing exploits against DSL Modems.

# Questions?

Thank you for joining me for this presentation.

Contact:

<https://twitter.com/nstarke>

<https://github.com/nstarke>

<https://secdsm.org> - @nstarke on SecDSM slack and #KernelCon slack