black hat®
USA 2023

AUGUST 9-10, 2023

BRIEFINGS

Route to Bugs: Analyzing the Security of BGP Message Parsing

Daniel dos Santos, Simon Guiot,

Stanislav Dashevskyi, Amine Amri, Oussama Kerro

Who We Are

- **Daniel dos Santos**, Head of Security Research
- **Simon Guiot**, Security Researcher

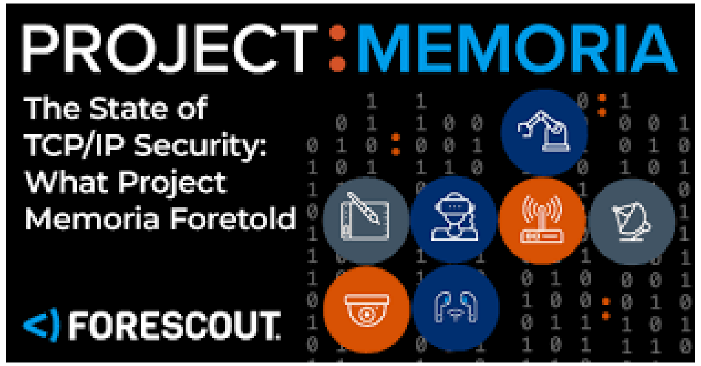
- **Stanislav Dashevskyi**, Principal Security Researcher
- **Amine Amri**, Security Researcher
- **Oussama Kerro**, Intern

FORESCOUT RESEARCH | VEDERE LABS

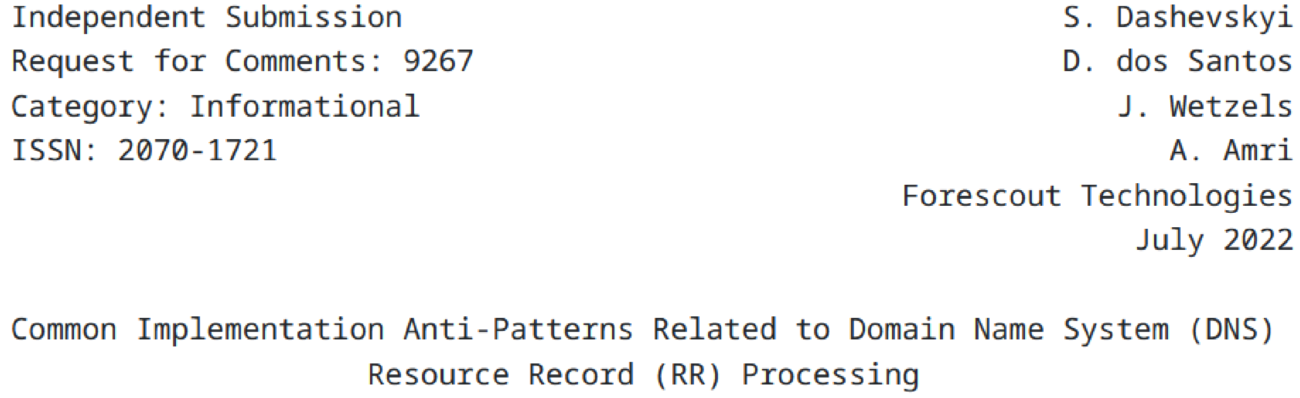
“At Forescout Vedere Labs we analyze the security implications of hyper connectivity and IT-OT convergence.”

Relevant Past Research

- **2020-21 Project Memoria** – large-scale analysis of embedded TCP/IP stacks
  - **AMNESIA:33** – 33 CVEs on 4 open-source stacks @ **Black Hat EU 2020**
  - **NUMBER:JACK** – 9 CVEs on TCP ISN
  - **NAME:WRECK** – 9 CVEs on DNS clients @ **Black Hat Asia 2021**
  - **INFRA:HALT** – 14 CVEs on a stack popular in OT @ **Hack in the Box 2021**
  - **NUCLEUS:13** – 13 CVEs on a stack popular in healthcare

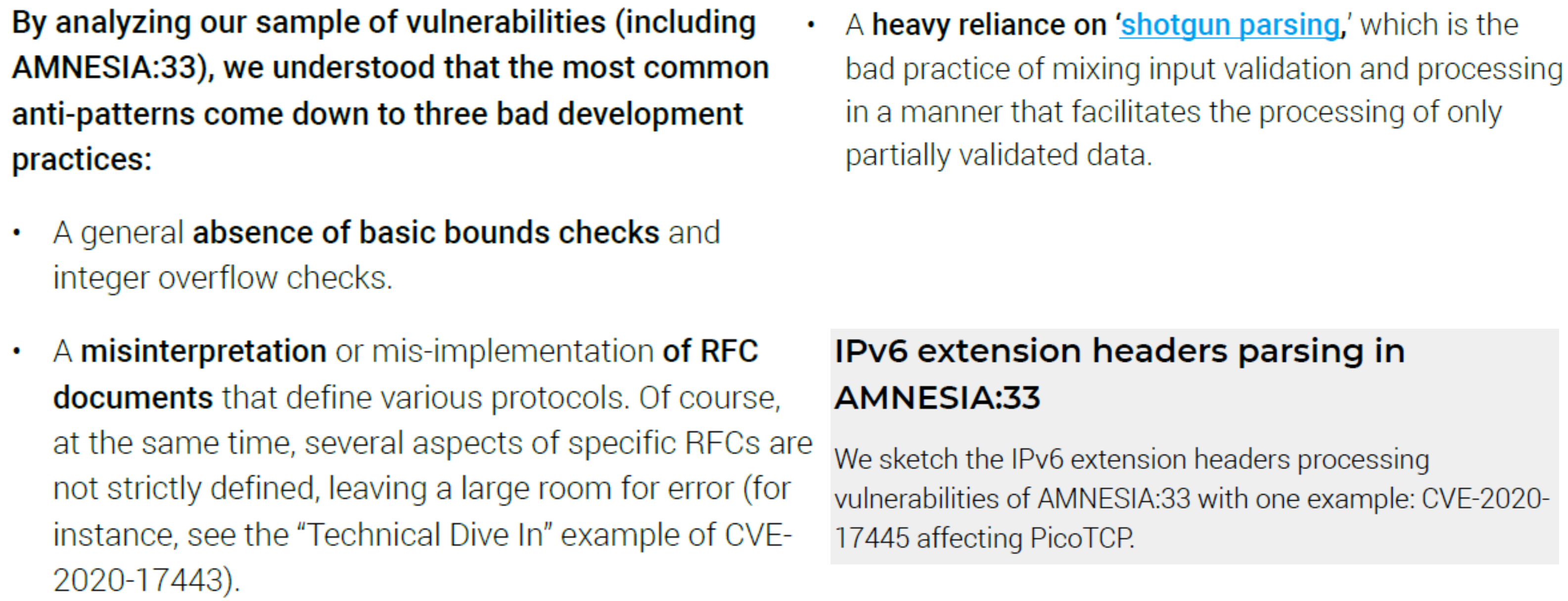


- Showed that different **implementations of the same protocol tend to fail the same way**



```
Independent Submission                                      S. Dashevskyi
Request for Comments: 9267                                   D. dos Santos
Category: Informational                                        J. Wetzels
ISSN: 2070-1721                                                   A. Amri
                                                   Forescout Technologies
                                                                July 2022


  Common Implementation Anti-Patterns Related to Domain Name System (DNS)
                      Resource Record (RR) Processing
```

https://datatracker.ietf.org/doc/rfc9267/



By analyzing our sample of vulnerabilities (including AMNESIA:33), we understood that the most common anti-patterns come down to three bad development practices:

- A general **absence of basic bounds checks** and integer overflow checks.
- A **misinterpretation** or mis-implementation **of RFC documents** that define various protocols. Of course, at the same time, several aspects of specific RFCs are not strictly defined, leaving a large room for error (for instance, see the "Technical Dive In" example of CVE-2020-17443).
- A **heavy reliance on '**shotgun parsing**,'** which is the bad practice of mixing input validation and processing in a manner that facilitates the processing of only partially validated data.

IPv6 extension headers parsing in AMNESIA:33

We sketch the IPv6 extension headers processing vulnerabilities of AMNESIA:33 with one example: CVE-2020-17445 affecting PicoTCP.

https://i.blackhat.com/eu-20/Wednesday/eu-20-dosSantos-How-Embedded-TCPIP-Stacks-Breed-Critical-Vulnerabilities-wp.pdf

Talk Summary

01

BGP is widely used

For Internet routing and other settings.

Most security research focuses on well-known issues of routing security instead of software vulnerabilities.

02

Implementations can also be vulnerable

Analyzed 4 closed source and 3 open-source implementations

Found permissive handling of messages and 3 new DoS vulnerabilities in a leading open-source implementation

Only TCP spoofing required to inject malformed packets in some cases

03

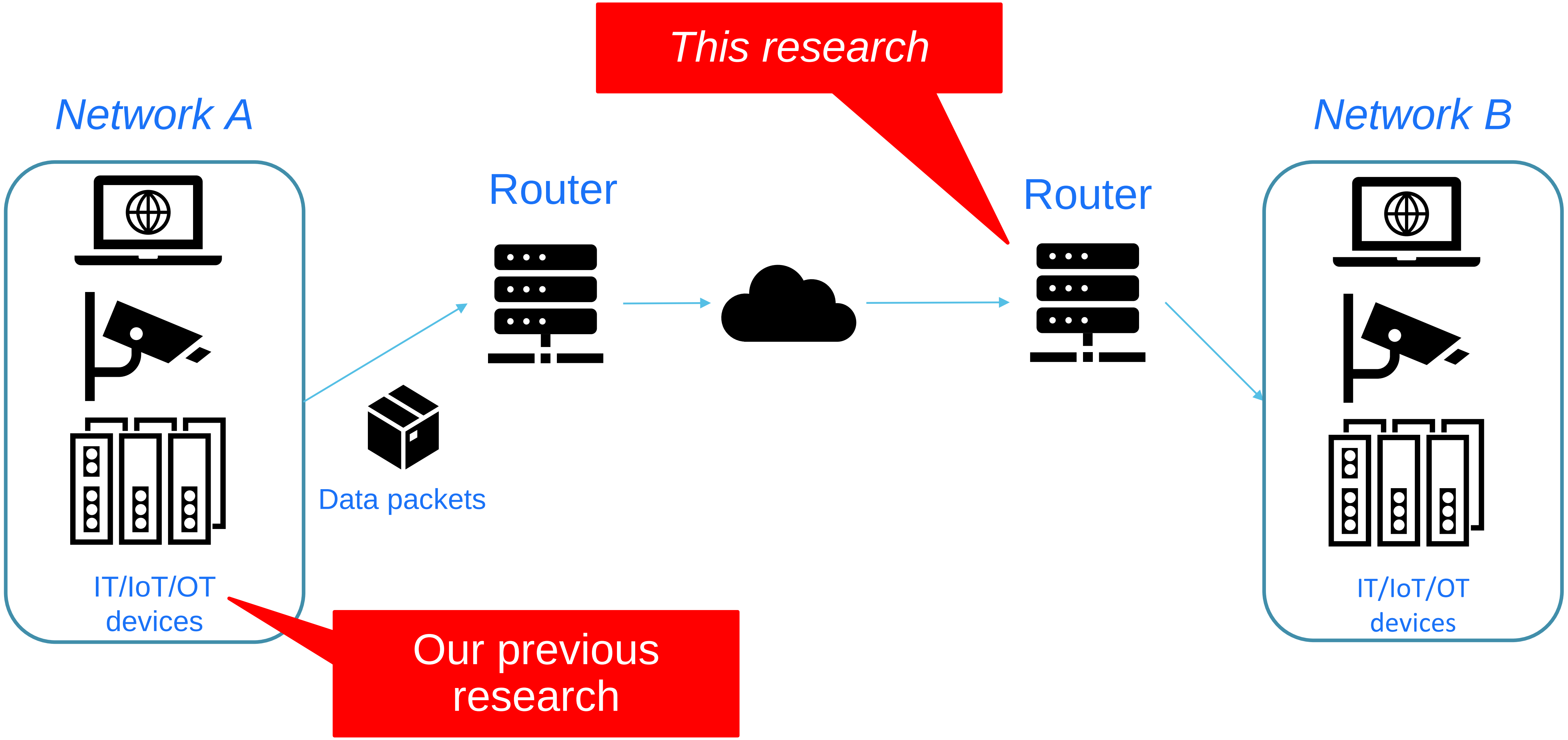
Conclusion

Pay attention to routing security, but don't forget about software vulnerabilities

Released a fuzzer and testing tool to help organizations test their deployments and researchers find new vulnerabilities

BGP

The Internet in a Nutshell

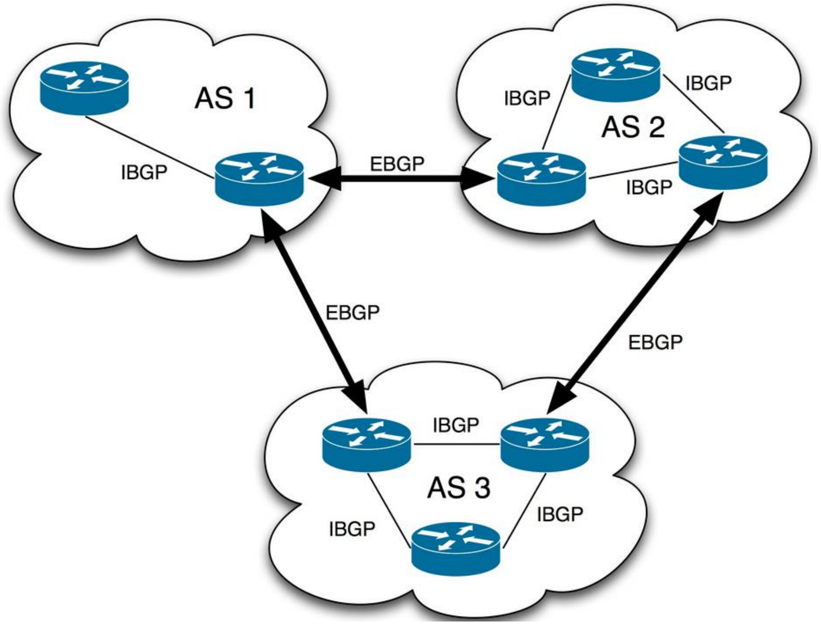


This research

Our previous research

What is BGP?

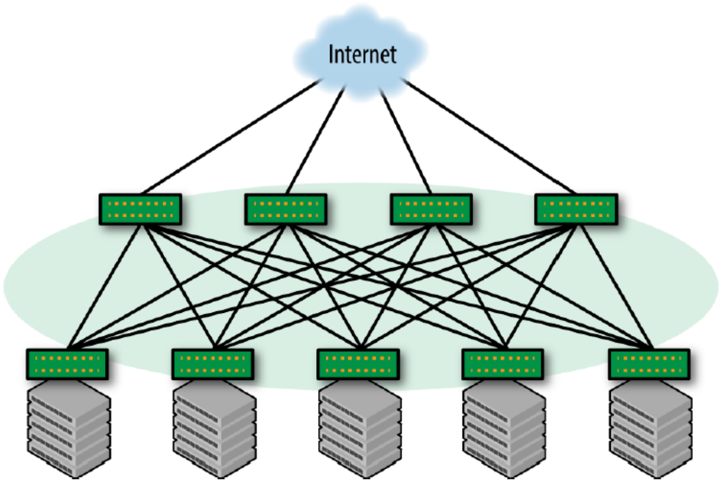
- **Routing for the Internet**
  - Protocol to exchange routing and reachability information among Autonomous Systems (AS)
  - AS is a block of IPs leased to an organization by a registrar (e.g., RIPE NCC) for a time period
  - BGP is used to advertise ASNs and peer networks that are considered each to be part of an AS
  - Internal BGP (peers within AS) and External BGP (peers on the Internet)
- **Makes routing decisions** based on paths, network policies, and rule-sets



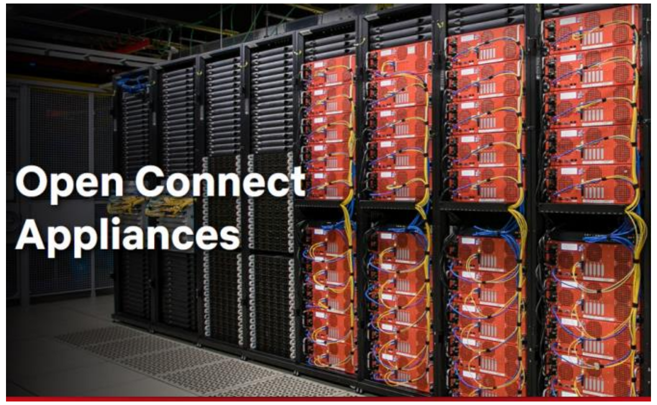
Routing Protocols Timeline

- 1982 – EGP
- 1985 – IGRP
- 1988 – RIPv1
- 1990 – IS-IS
- 1991 – OSPFv2
- 1992 – EIGRP
- 1994 – RIPv2
- 1995 – BGP
- 1997 – RIPng
- 1999 – BGPv6 and OSPFv3
- 2000 – IS-ISv6

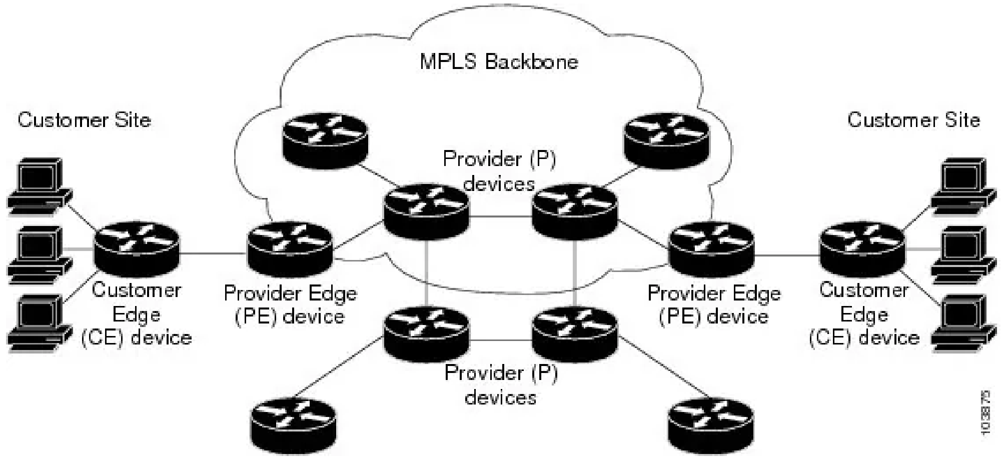
Other use cases



Internal data center routing



Embedded in custom appliances


MPLS Backbone
Customer Site
Customer Site
Provider (P) devices
Customer Edge (CE) device
Provider Edge (PE) device
Provider Edge (PE) device
Customer Edge (CE) device
Provider (P) devices
103875

MPLS VPN across organization sites

MetalLB

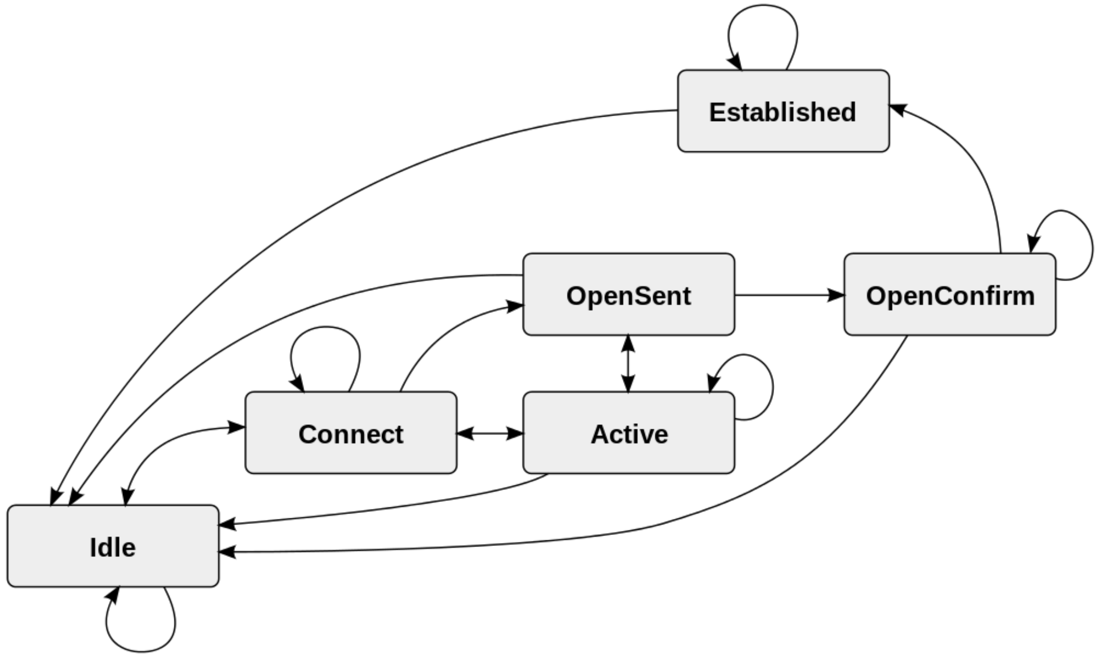
Kubernetes load balancing

…

In summary: BGP security is not just for ISPs and IXes

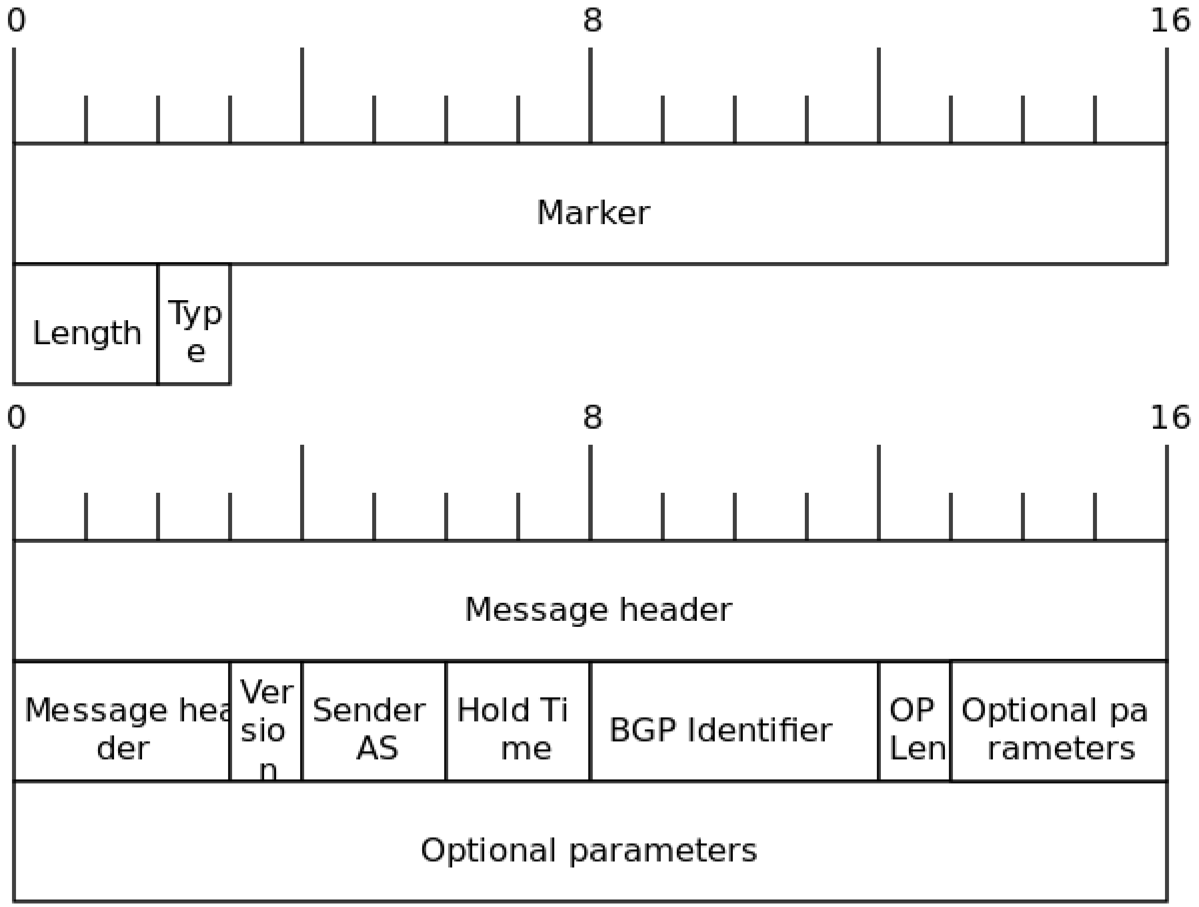
BGP Basics

Simple state machine



Limited set of messages: OPEN, UPDATE, NOTIFICATION, KEEPALIVE

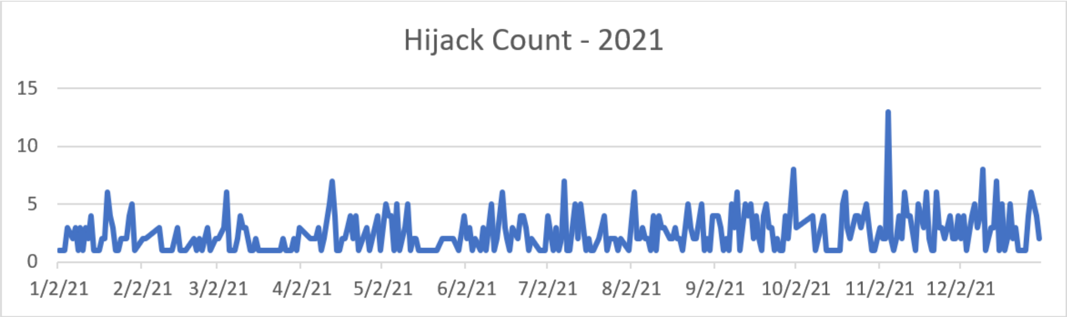
Relatively **straightforward** packets

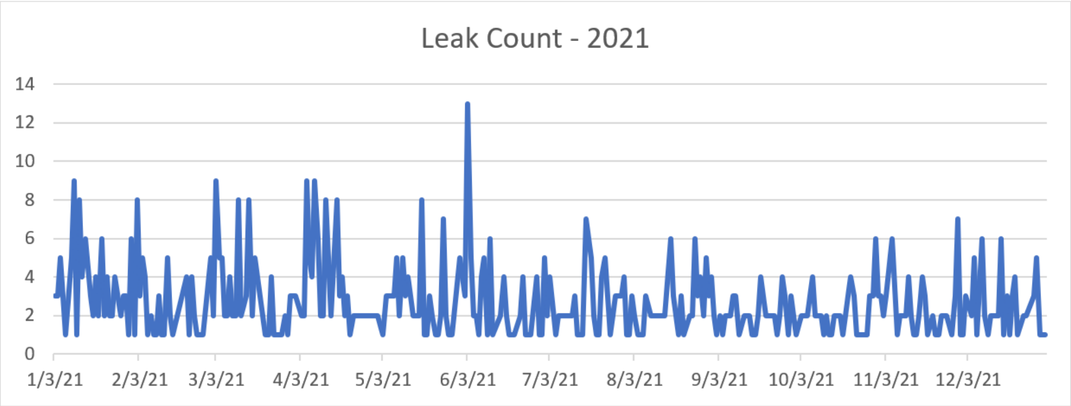


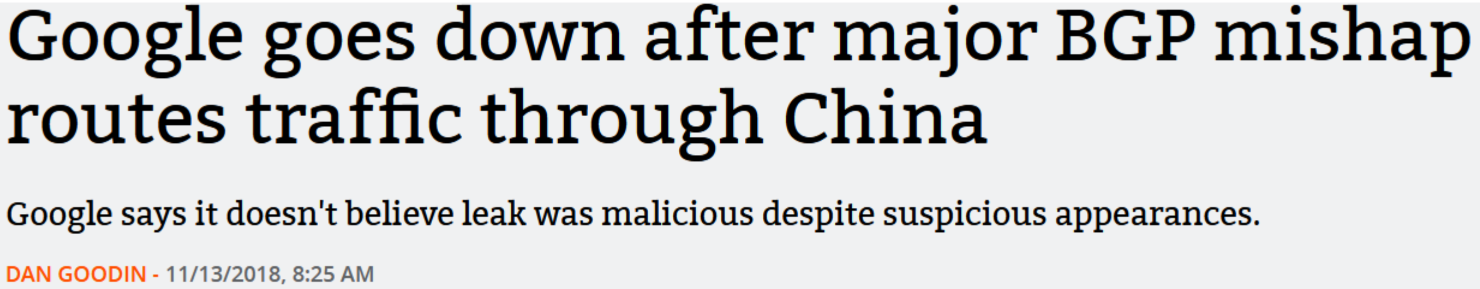
What could go wrong?

When BGP Fails

- BGP has **no built-in security**, such as an authentication and authorization mechanism
- **Mistakes or intentional attacks** lead to **network outages and traffic redirection**
  - Hijacks – when a network originates a prefix owned by another network without permission
  - Leaks – when a network propagates a routing announcement beyond its intended scope
- Issues **known for a long time but still *thousands* of incidents per year**



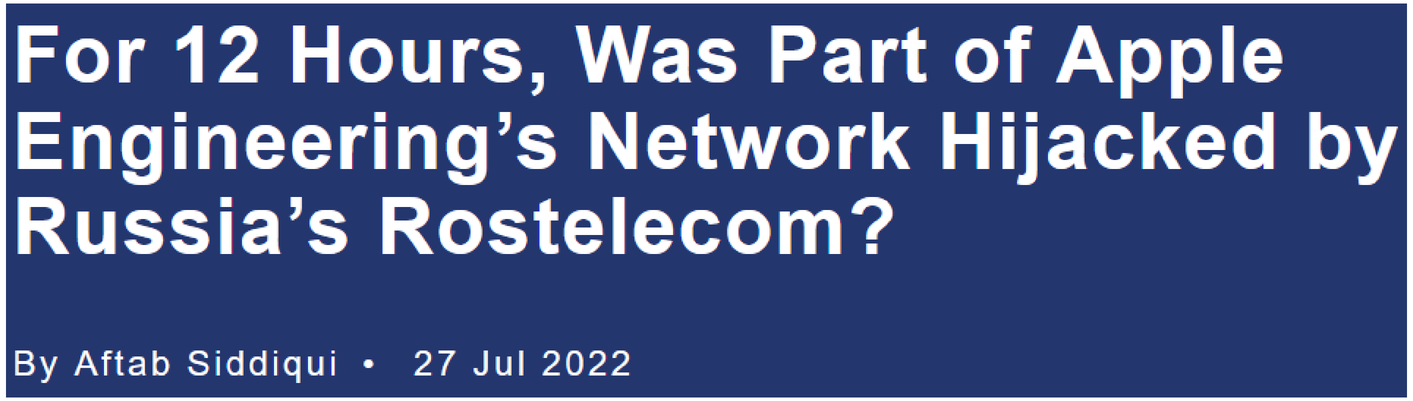




Google goes down after major BGP mishap routes traffic through China

Google says it doesn't believe leak was malicious despite suspicious appearances.

DAN GOODIN - 11/13/2018, 8:25 AM



For 12 Hours, Was Part of Apple Engineering's Network Hijacked by Russia's Rostelecom?

By Aftab Siddiqui • 27 Jul 2022

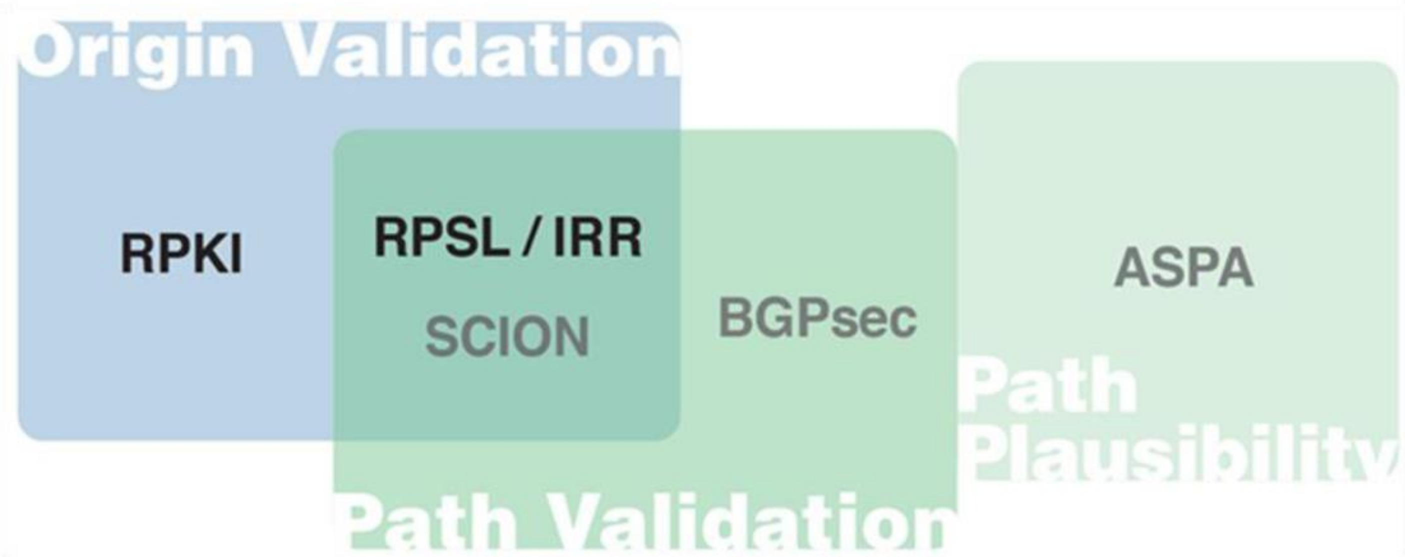
https://www.manrs.org t.ly/3Zc6

Traditional BGP Security

- **RFC4272**: BGP Security Vulnerabilities Analysis (2006)

- Main concern is to **filter incorrect or malicious routing information**
  - **Origin** validation – verify that a network announcing a route is authorized to do it
  - **Path** validation – ensure that no unauthorized network has diverted traffic by a false route
  - Path plausibility – determine the plausibility of a network included in the AS path

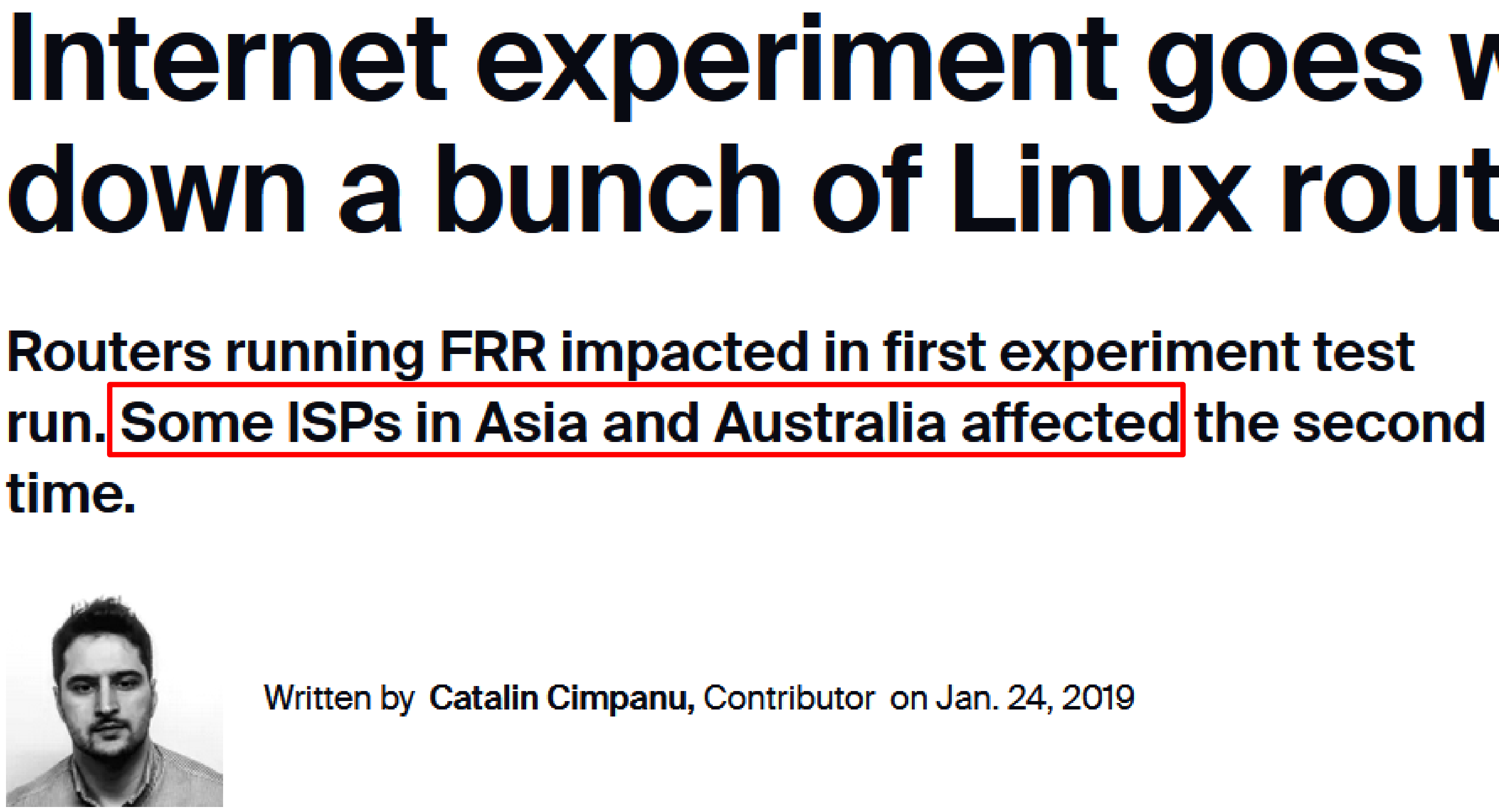
Figure 5. Mapping of current routing security techniques



https://doi.org/10.1787/20716826

- *What about vulnerabilities in **BGP implementations**?*

When BGP Fails Because of Software Flaws

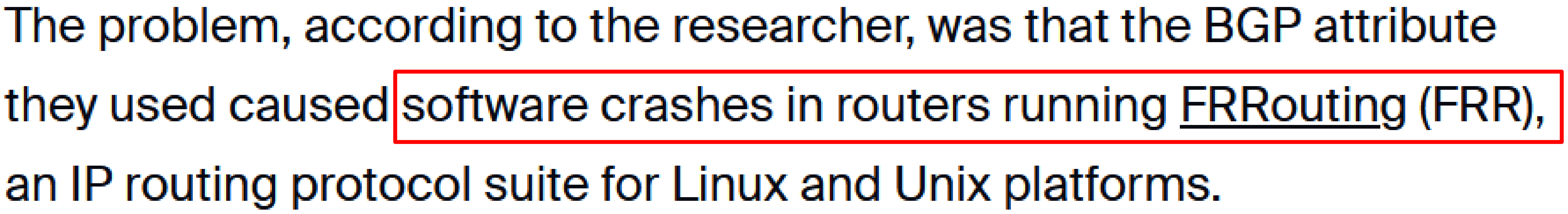


Internet experiment goes wrong, takes down a bunch of Linux routers

Routers running FRR impacted in first experiment test run. Some ISPs in Asia and Australia affected the second time.

Written by **Catalin Cimpanu,** Contributor on Jan. 24, 2019

FRROUTING



The problem, according to the researcher, was that the BGP attribute they used caused software crashes in routers running FRRouting (FRR), an IP routing protocol suite for Linux and Unix platforms.

https://www.zdnet.com/article/internet-experiment-goes-wrong-takes-down-a-bunch-of-linux-routers/

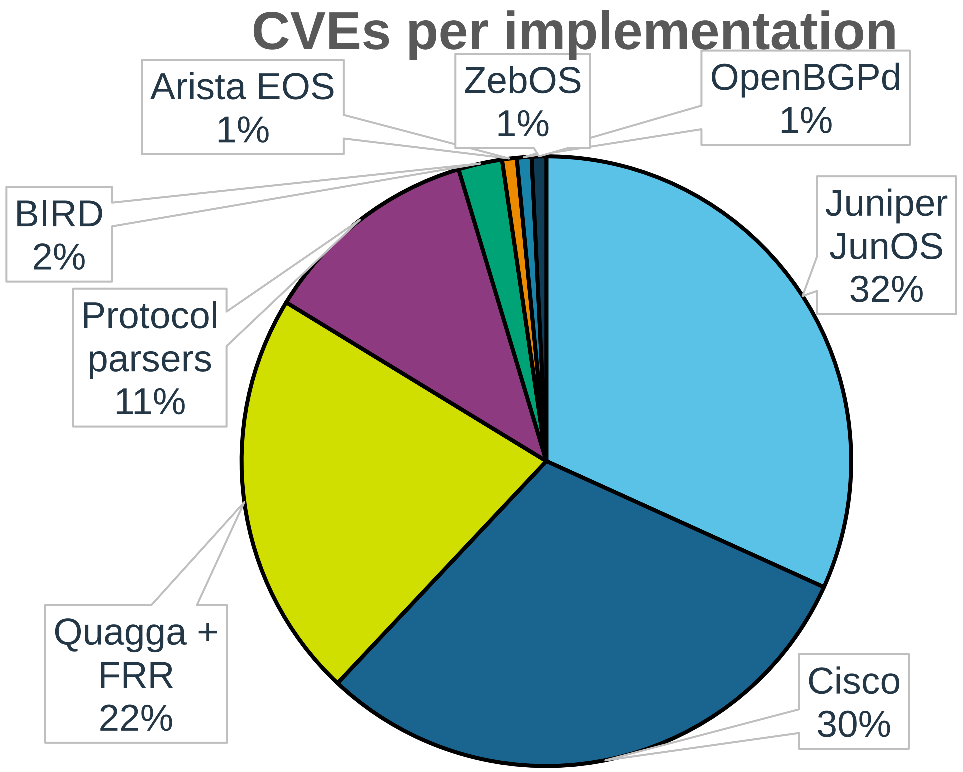
Why Research BGP implementations?

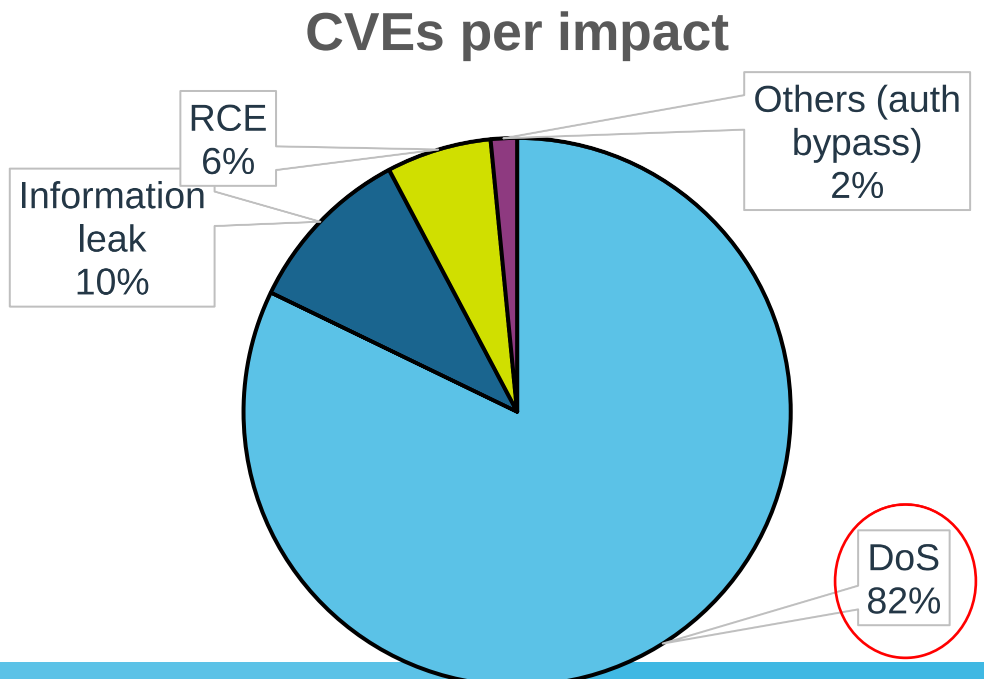
- **Latest systematized** work we found about testing BGP implementations was **20 years ago**
  - https://www.blackhat.com/presentations/bh-usa-03/bh-us-03-convery-franz-v3.pdf
  - Team at Cisco looked at implementation and configuration of BGP across vendors
  - Created a fuzzer, analyzed 7 implementations and found 4 new CVEs
  - Concluded that misconfigurations were more dangerous than implementation issues

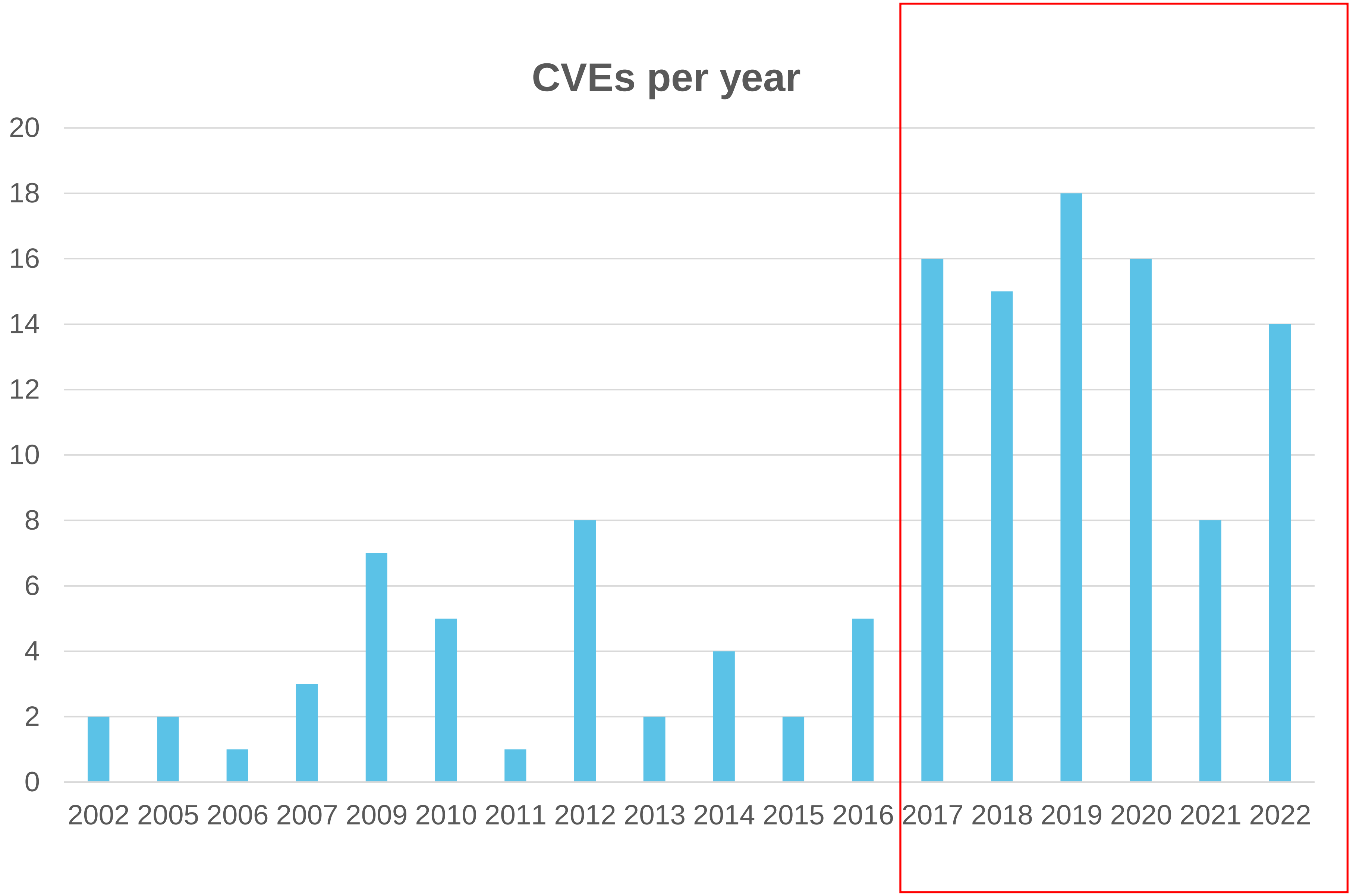
- **In 2007**, team at Juniper analyzed **UPDATE message handling** in several vendors
  - https://www.kb.cert.org/vuls/id/929656
  - Mishandling could lead to DoS
  - 7 vendors affected, 10 not affected, 25 unknown

- In the meantime, **129 CVEs** on BGP implementations, including **RCEs**
  - 123 (95%) because of message parsing issues

Previous Vulnerabilities







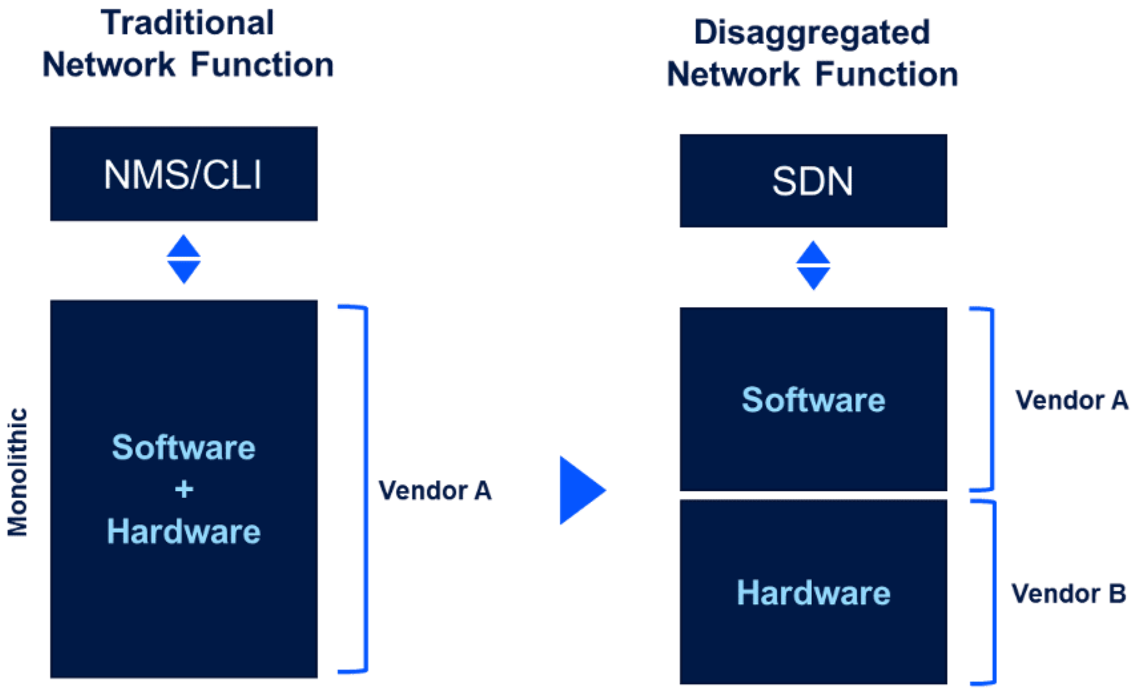
Current Threat Landscape

- **Threat actors focusing on network infrastructure**
  - China: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a
  - Russia: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108
  - Ransomware groups, other cybercriminals, hacktivists, …
  - Recent CISA BOD 23-02: https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02

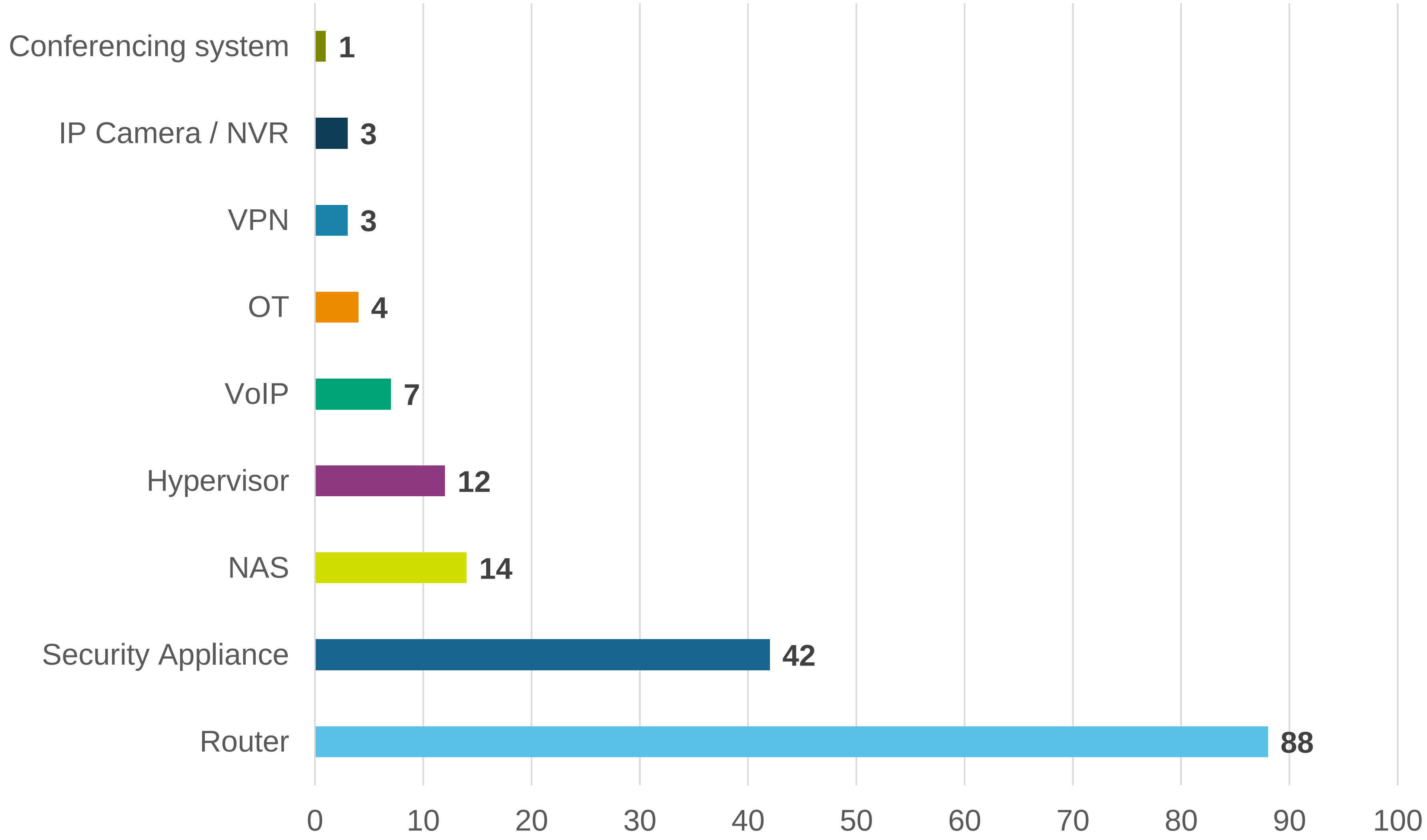
- Still **several BGP implementations** were not systematically analyzed

- **Open BGP implementations** are gaining traction with NFD

- Many different implementations of *routing platforms, network operating systems, looking glass servers* and other **routing components.** We catalogued:
  - 52 routing protocols, 40 open
  - 20 routing platforms, 17 open
  - 53 Network Operating Systems, 20 open



Known Exploited Vulnerabilities *Routers*



- CISA tracks 925 known exploited vulnerabilities (May 2023)
- Most affect IT software, but 179 can be mapped to specific devices
- Of those, 88 (49%) target *routers*
- See (Shandilya, VB2019) as to why https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Shandilya.pdf

Based on data from https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Known Exploited Vulnerabilities *BGP*

Out of those 88, **3 decades-old CVEs affecting Cisco BGP being exploited in 2022**:

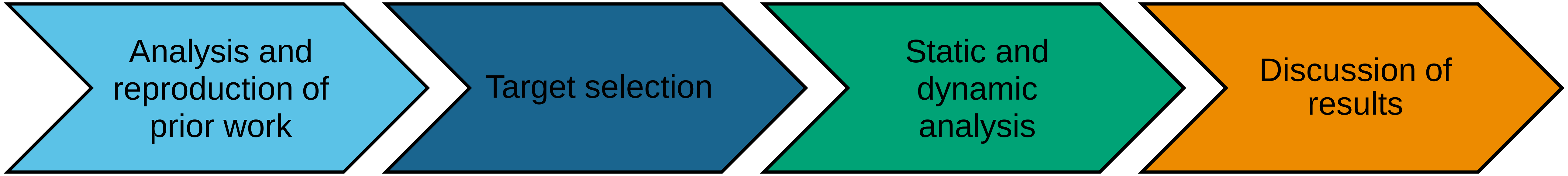
CVE ID	Vendor	Product	Description	Impact	Date Added
CVE-2010-3035	Cisco	IOS XR	Cisco IOS XR, when BGP is the configured routing feature, allows remote attackers to cause a denial-of-service.	DoS	2022-03-25
CVE-2009-2055	Cisco	IOS XR	Out-of-bounds read when processing a malformed BGP OPEN message with an Extended Optional Parameters Length option. This is a different issue from CVE-2022-40302.	DoS	2022-03-25
CVE-2017-12319	Cisco	IOS XE	Out-of-bounds read when processing a malformed BGP OPEN message that abruptly ends with the option length octet (or the option length word, in case of OPEN with extended option lengths message).	DoS	2022-03-03

Also 2 other DoS on Cisco IOS XR routing: CVE-2020-3566 and CVE-2020-2569 affecting DVMRP

Based on data from https://www.cisa.gov/known-exploited-vulnerabilities-catalog black hat USA 2023

Finding Vulnerabilities

Methodology



Analysis and reproduction of prior work

Target selection

Static and dynamic analysis

Discussion of results

- **Prior work discussed in the previous section**

- **Target selection**
  - All implementations with published vulnerabilities + Mikrotik - ZebOS (== *most popular implementations*)
  - 3 open source: FRRouting, BIRD, OpenBGPd
  - 4 closed source: Mikrotik RouterOS, Juniper JunOS, Cisco IOS, Arista EOS

- **Static and dynamic analysis**
  - Anti-patterns and strategies derived from RFCs + previous vulnerabilities + previous experience with protocol parsing
  - Reverse engineering for closed-source implementations
  - Specific black-box fuzzers for each message type

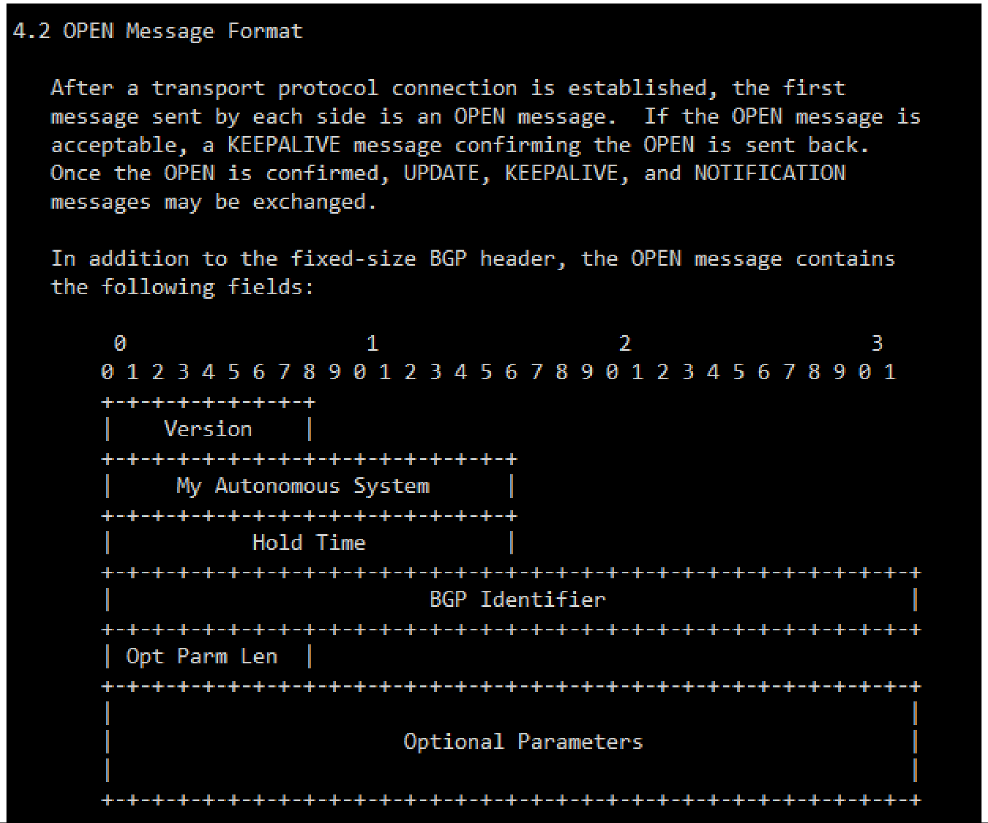
- **Results in the next slides**

Manual analysis
Anti-patterns

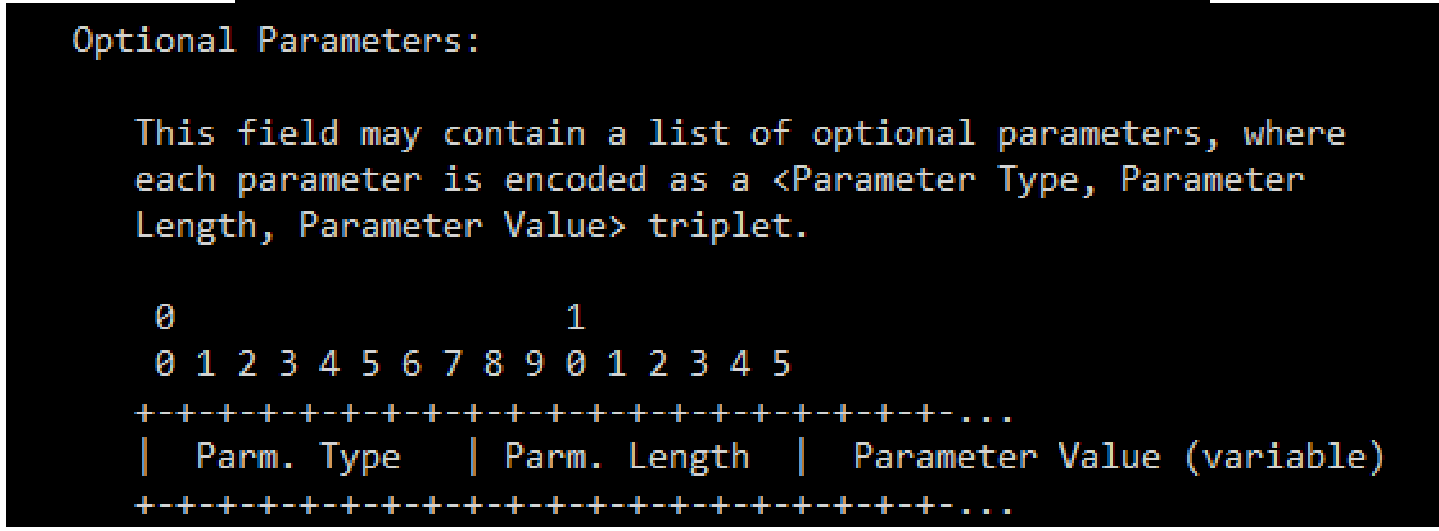
- **Distilled anti-patterns**
  1. **Type-Length-Value** fields in BGP messages
  2. **Optional TLV parameters** in OPEN messages
  3. **Route/path length fields** in UPDATE messages

  4. Peer **responds to any OPEN** message
  5. Peer **accepts UPDATE messages** without exchanging OPEN messages
  6. Handling of **BGP extensions**

- **Results:** no CVE found by manual analysis, BUT…



```
4.2 OPEN Message Format

   After a transport protocol connection is established, the first
   message sent by each side is an OPEN message.  If the OPEN message is
   acceptable, a KEEPALIVE message confirming the OPEN is sent back.
   Once the OPEN is confirmed, UPDATE, KEEPALIVE, and NOTIFICATION
   messages may be exchanged.

   In addition to the fixed-size BGP header, the OPEN message contains
   the following fields:

        0                   1                   2                   3
       0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
       +-+-+-+-+-+-+-+-+
       |    Version    |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |     My Autonomous System      |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |           Hold Time           |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                         BGP Identifier                        |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       | Opt Parm Len  |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                                                               |
       |             Optional Parameters                               |
       |                                                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
Optional Parameters:

   This field may contain a list of optional parameters, where
   each parameter is encoded as a <Parameter Type, Parameter
   Length, Parameter Value> triplet.

    0                   1
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
   |  Parm. Type   | Parm. Length  |  Parameter Value (variable)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
```

Results
Handling of OPEN responses

Implementation	Description
FRRouting	Proceeds with a TCP handshake, terminates the TCP session (TCP Reset packet) after an OPEN packet is received. Performs some processing of OPEN messages, before validating the BGP ID and ASN fields.
BIRD	Proceeds with a TCP handshake, terminates the TCP session (TCP Reset packet) after an OPEN packet is received.
OpenBGPd	
Mikrotik RouterOS	
Arista EOS	
Juniper JunOS	Proceeds with a TCP handshake. Sends back an OPEN message, sends back a Cease NOTIFICATION message with the subcode 5 (Connection Rejected).
Cisco IOS	Does not allow to establish a TCP connection (TCP handshake fails).

- Most implementations proceed with TCP handshake before checking if OPEN message comes from pre-configured peer because the BGP daemon runs in user mode (except for Cisco IOS)
- Connection filtering not happening on the kernel level

- **FRRouting decapsulates optional parameters** before verifying BGP ID and ASN fields, which means that attackers only need to spoof the originating IP address

Fuzzing

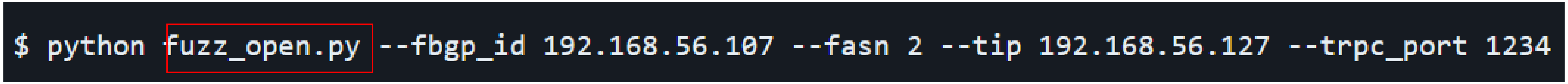
- **Could not find open BGP fuzzer, so developed our own**

- **Stateful fuzzer that will:**
  - Establish a session with a peer
  - Run test cases based on the anti-patterns we defined
  - For each test case, send malformed message with specific payload (based on boofuzz)
    - OPEN, UPDATE, ROUTE REFRESH, NOTIFICATION
  - Test the target for crashes via a custom RPC monitor (based on boofuzz procmon)

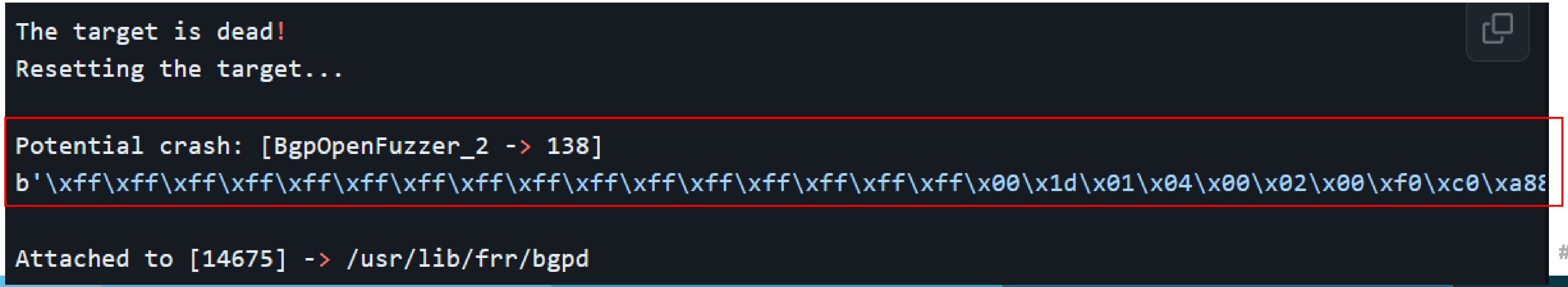
boofuzz

Thanks to Joshua Pereyda and the BooFuzz contributors.

- **Freely available** on https://github.com/Forescout/bgp_boofuzzer
  - Lots of opportunities to improve it – please contribute!

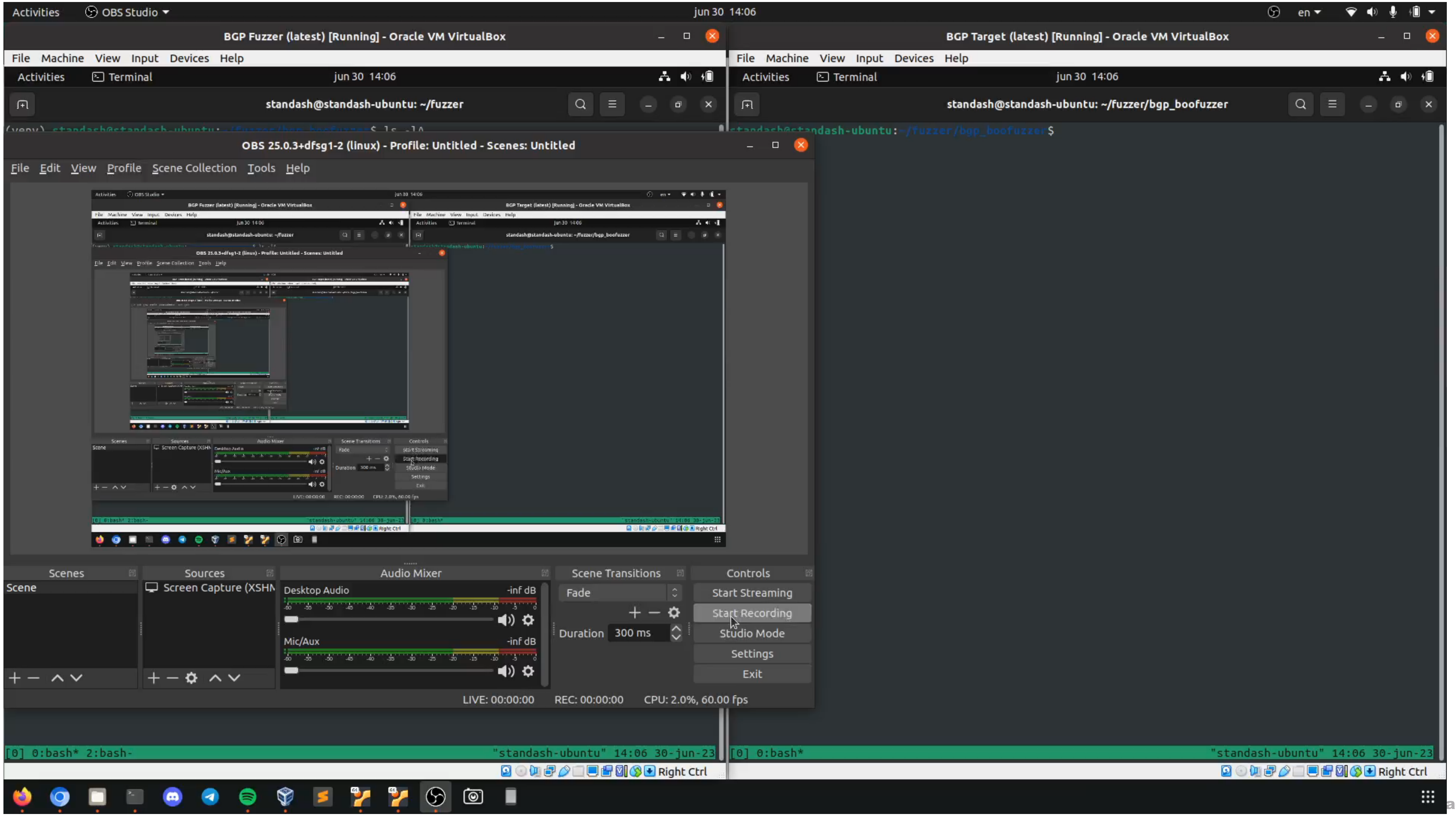


```
$ python fuzz_open.py --fbgp_id 192.168.56.107 --fasn 2 --tip 192.168.56.127 --trpc_port 1234
```



```
The target is dead!
Resetting the target...

Potential crash: [BgpOpenFuzzer_2 -> 138]
b'\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\xff\x00\x1d\x01\x04\x00\x02\x00\xf0\xc0\xa8

Attached to [14675] -> /usr/lib/frr/bgpd
```

Fuzzing demo



Activities
OBS Studio
jun 30 14:06
en
BGP Fuzzer (latest) [Running] - Oracle VM VirtualBox
BGP Target (latest) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal jun 30 14:06
standash@standash-ubuntu: ~/fuzzer
standash@standash-ubuntu: ~/fuzzer/bgp_boofuzzer
OBS 25.0.3+dfsg1-2 (linux) - Profile: Untitled - Scenes: Untitled
File Edit View Profile Scene Collection Tools Help
Scenes
Scene
Sources
Screen Capture (XSHN
Audio Mixer
Desktop Audio -inf dB
Mic/Aux -inf dB
Scene Transitions
Fade
Duration 300 ms
Controls
Start Streaming
Start Recording
Studio Mode
Settings
Exit
LIVE: 00:00:00 REC: 00:00:00 CPU: 2.0%, 60.00 fps
Right Ctrl

```
(venv) standash@standash-ubuntu:~/fuzzer/bgp_boofuzzer$ ls -lA
```

```
[0] 0:bash* 2:bash-                "standash-ubuntu" 14:06 30-jun-23
```

```
standash@standash-ubuntu:~/fuzzer/bgp_boofuzzer$
```

```
[0] 0:bash*                        "standash-ubuntu" 14:06 30-jun-23
```

Results
New CVEs

CVE ID	Tested Product	Description	Potential Impact
CVE-2022-40302	FRRouting 8.4	Out-of-bounds read when processing a malformed BGP OPEN message with an Extended Optional Parameters Length option.	DoS
CVE-2022-40318	FRRouting 8.4	Out-of-bounds read when processing a malformed BGP OPEN message with an Extended Optional Parameters Length option. This is a different issue from CVE-2022-40302.	DoS
CVE-2022-43681	FRRouting 8.4	Out-of-bounds read when processing a malformed BGP OPEN message that abruptly ends with the option length octet (or the option length word, in case of OPEN with extended option lengths message).	DoS

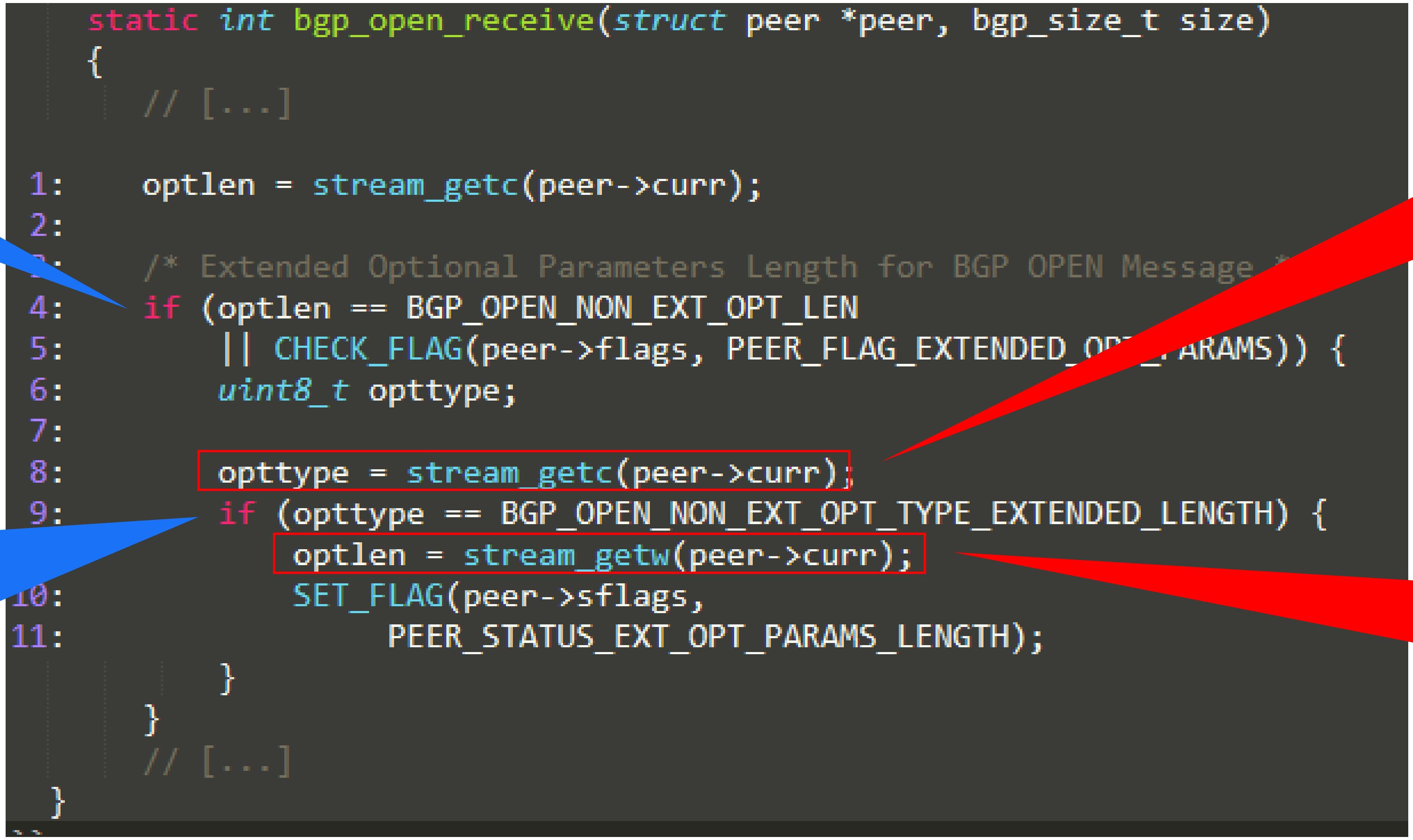
- Very low hanging fruits – found quickly by the fuzzer
- Very similar to the Cisco IOS XR issues being currently exploited
- Issues reported to the FRRouting team and fixed *very* quickly (same day in some cases)

CVE-2022-43681

Root cause: Insufficient bounds checks of extended option length octets in OPEN messages

If option length octet == 0xff, then read the next octet (*opttype*)

If opttype == 0xff, the msg contains extended optional params, then read next word (*optlen*)



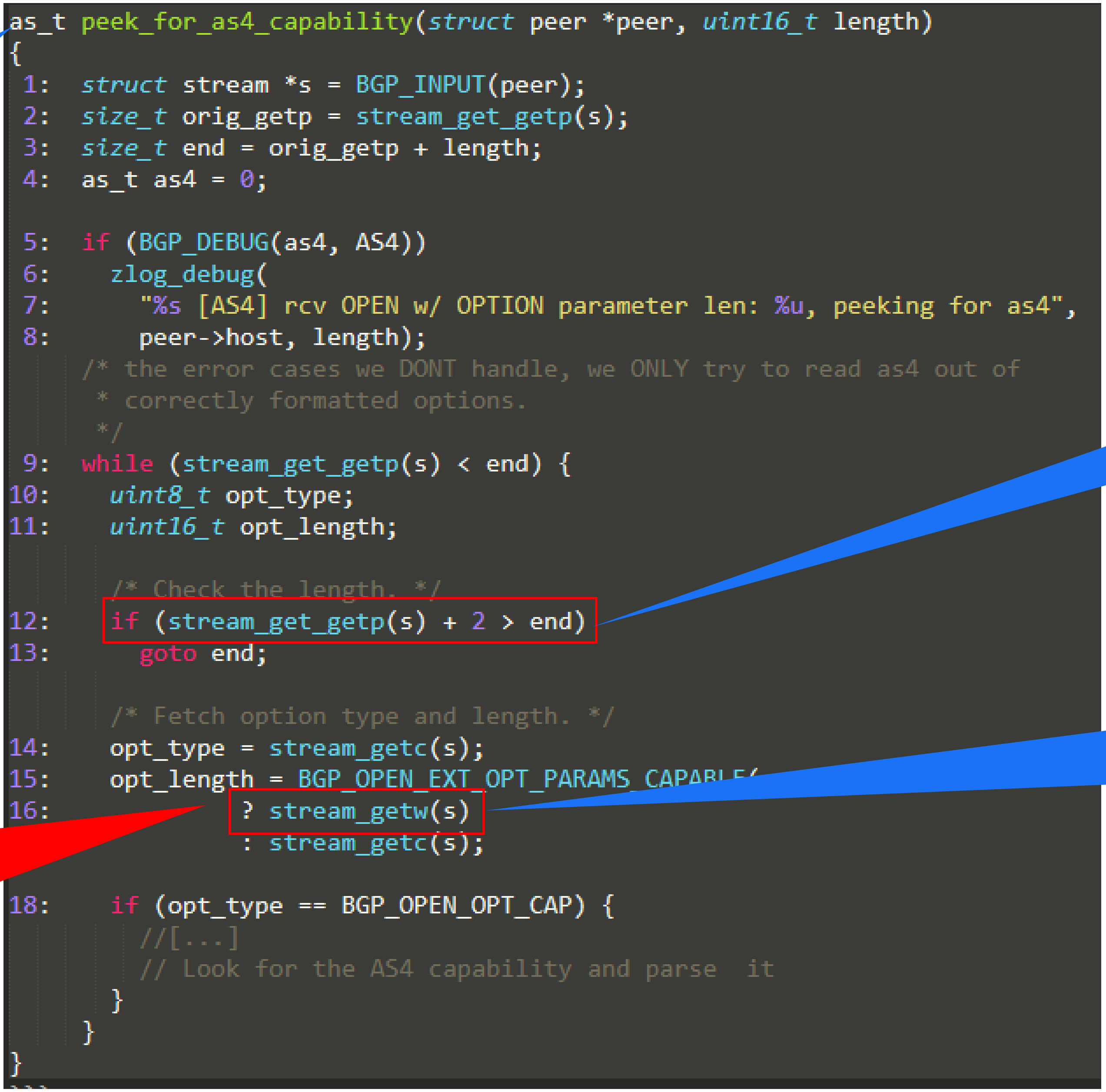
```
static int bgp_open_receive(struct peer *peer, bgp_size_t size)
{
    // [...]

    optlen = stream_getc(peer->curr);

    /* Extended Optional Parameters Length for BGP OPEN Message */
    if (optlen == BGP_OPEN_NON_EXT_OPT_LEN
        || CHECK_FLAG(peer->flags, PEER_FLAG_EXTENDED_OPT_PARAMS)) {
        uint8_t opttype;

        opttype = stream_getc(peer->curr);
        if (opttype == BGP_OPEN_NON_EXT_OPT_TYPE_EXTENDED_LENGTH) {
            optlen = stream_getw(peer->curr);
            SET_FLAG(peer->sflags,
                     PEER_STATUS_EXT_OPT_PARAMS_LENGTH);
        }
    }
    // [...]
}
```

If malformed message ends with one 0xff, this call will read 1 octet beyond packet

If malformed message ends with two 0xff, this call will read 1 word beyond packet

CVE-2022-40302

Root cause: Insufficient bounds checks when reading the AS4 capability of OPEN messages



```
as_t peek_for_as4_capability(struct peer *peer, uint16_t length)
{
 1:   struct stream *s = BGP_INPUT(peer);
 2:   size_t orig_getp = stream_get_getp(s);
 3:   size_t end = orig_getp + length;
 4:   as_t as4 = 0;

 5:   if (BGP_DEBUG(as4, AS4))
 6:     zlog_debug(
 7:       "%s [AS4] rcv OPEN w/ OPTION parameter len: %u, peeking for as4",
 8:       peer->host, length);
      /* the error cases we DONT handle, we ONLY try to read as4 out of
       * correctly formatted options.
       */
 9:   while (stream_get_getp(s) < end) {
10:     uint8_t opt_type;
11:     uint16_t opt_length;

        /* Check the length. */
12:     if (stream_get_getp(s) + 2 > end)
13:       goto end;

        /* Fetch option type and length. */
14:     opt_type = stream_getc(s);
15:     opt_length = BGP_OPEN_EXT_OPT_PARAMS_CAPABLE(
16:                    ? stream_getw(s)
                       : stream_getc(s);

18:     if (opt_type == BGP_OPEN_OPT_CAP) {
          //[...]
          // Look for the AS4 capability and parse  it
        }
      }
}
```

Function called before processing other options. *Iterates over all options to find and parse AS4 capability.*

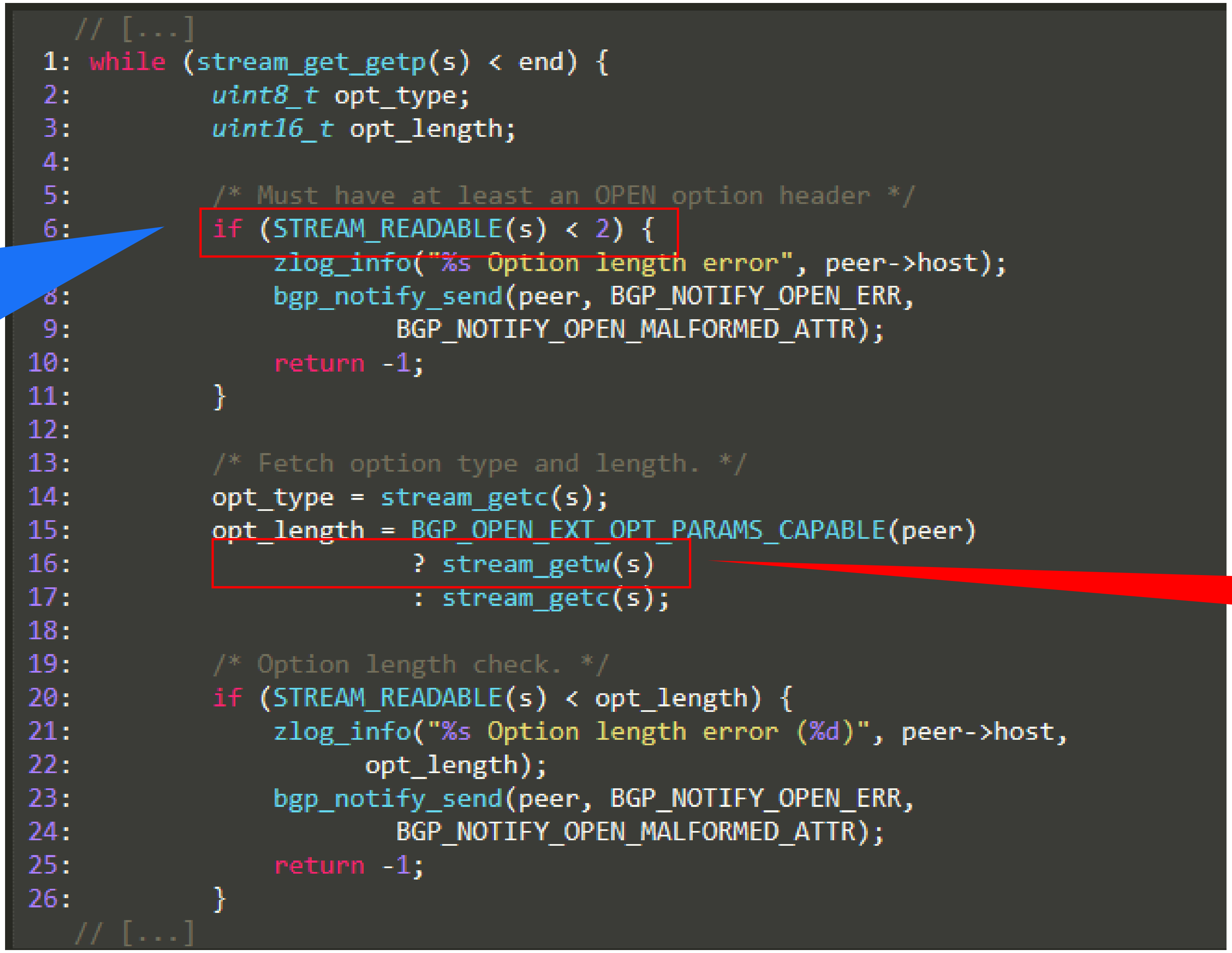
Checks for 2 bytes against received option length

If message has optional parameters with extended length, read 3 bytes

Attacker can craft packet that passes check on line 12 and reaches here, reading 1 byte out-of-bounds

CVE-2022-40318

Root cause: Similar to previous one, but goes through *peek_for_as4_capability()* and triggered later in *bgp_open_option_parse()*



```
// [...]
while (stream_get_getp(s) < end) {
        uint8_t opt_type;
        uint16_t opt_length;

        /* Must have at least an OPEN option header */
        if (STREAM_READABLE(s) < 2) {
            zlog_info("%s Option length error", peer->host);
            bgp_notify_send(peer, BGP_NOTIFY_OPEN_ERR,
                    BGP_NOTIFY_OPEN_MALFORMED_ATTR);
            return -1;
        }

        /* Fetch option type and length. */
        opt_type = stream_getc(s);
        opt_length = BGP_OPEN_EXT_OPT_PARAMS_CAPABLE(peer)
                     ? stream_getw(s)
                     : stream_getc(s);

        /* Option length check. */
        if (STREAM_READABLE(s) < opt_length) {
            zlog_info("%s Option length error (%d)", peer->host,
                  opt_length);
            bgp_notify_send(peer, BGP_NOTIFY_OPEN_ERR,
                    BGP_NOTIFY_OPEN_MALFORMED_ATTR);
            return -1;
        }
// [...]
```

Again, accounts for 2 octets in a packet with regular option length

Fails to account for extended option lengths (3 octets)

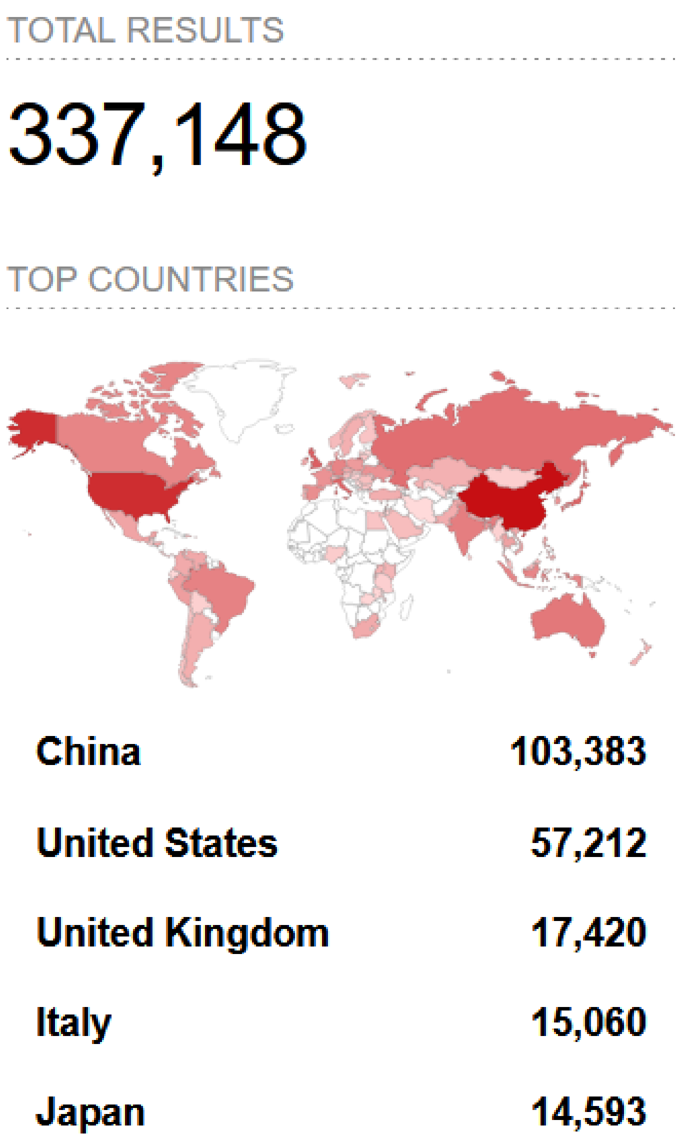
Read out of bounds here

black hat USA 2023

Conclusion

Impact Summary

- **Any of the 3 new CVEs leads to DoS on a vulnerable BGP peer**
  - Dropping all BGP sessions and routing tables and rendering the peer unresponsive for several seconds
  - BGP service will automatically restart after a timeout
  - DoS may be prolonged indefinitely by repeatedly sending malformed packets
- **Two issues can be triggered before FRRouting validates BGP Identifier and ASN fields**
  - In this case attackers only need to spoof a valid IP address of a trusted peer
- **Beyond these vulnerabilities**
  - More than 330,000 hosts with BGP enabled on the Internet
  - More than 200,000 hosts running Quagga (project from which FRR is forked)
  - More than 1,000 hosts running FRRouting



TOTAL RESULTS

337,148

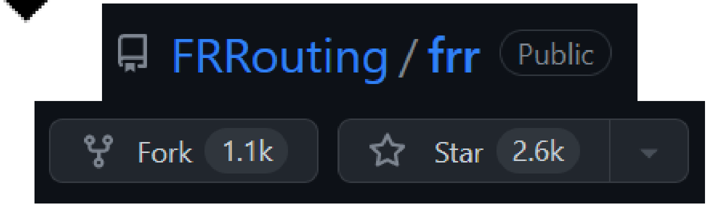
TOP COUNTRIES

China	103,383
United States	57,212
United Kingdom	17,420
Italy	15,060
Japan	14,593

Supply Chain Issues

FRROUTING

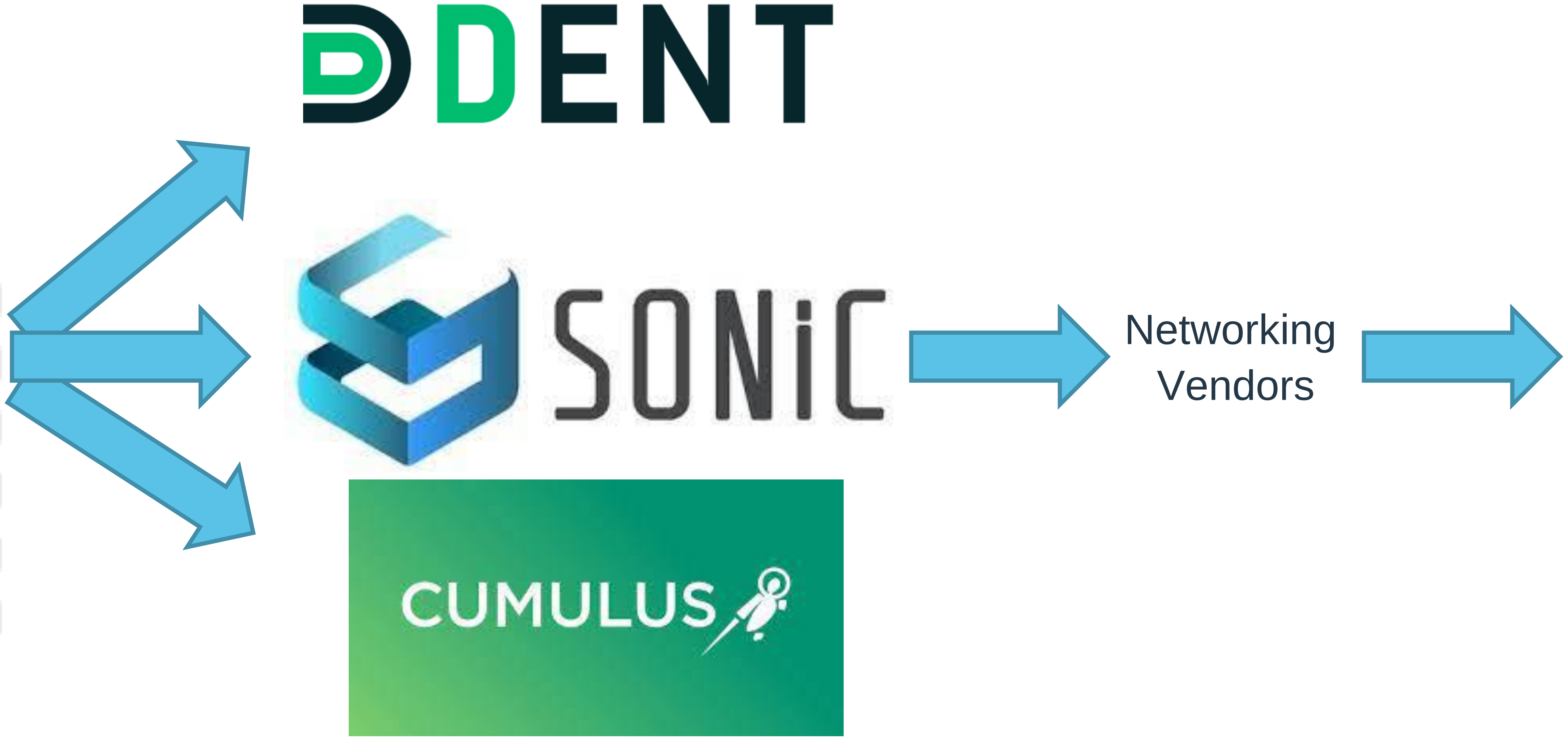
- 1996 • Zebra is created
- 2002 • Quagga is created
- 2016 • FRR forks from Quagga
- 2019 • Amazon DENT announced with FRR
- 2019 • Microsoft SONiC adopts FRR
- 2020 • FRR 7.4 is released



FRRouting / frr Public

Fork 1.1k Star 2.6k

Open-source routing platform (1k+ forks)



Networking OSes

https://www.nextplatform.com/2020/10/26/frr-the-most-popular-network-router-youve-never-heard-of/

Risk Mitigation

- Routing security is **still very important. Several good guides:**
  - Mutually Agreed Norms for Routing Security (MANRS)
  - RFC7454 – BGP Operations and Security
  - NIST SP800-189 Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation
  - *Many others…*

MANRS

www.manrs.org

- But threat actors have been attacking networking infrastructure devices directly
  - **Don’t forget software vulnerabilities** and securing networking devices
  - Identify all devices in your network that may be using BGP
  - Assess vulnerabilities and patch when possible

- Fuzzer we released comes with prepared test-cases for the CVEs we found to be tested against your network

Takeaways & Future Work

- **Takeaways**
  - BGP is crucial for the Internet and widely used beyond ISPs and IXes
  - Unlike embedded TCP/IP stacks, BGP implementations have matured and in general do not have obvious mistakes, but popular BGP implementations still have vulnerabilities or are too permissive
  - Network Function Disaggregation will make some open implementations very popular – it's important to keep the security of these projects in check.
  - Threat actors are exploiting these kinds of issues
  - Mitigation should not be only about routing security and is not entirely up to your ISP

https://www.forescout.com/resources/analyzing-the-security-of-bgp-message-parsing/

- **Future work**
  - Keep fuzzing new versions and new implementations – improve the fuzzer with new test cases
  - Explore other parts of the routing attack surface: other routing protocols, looking glass servers, remote control (e.g., Quagga VTY)

Thank you!

https://www.forescout.com/research-labs-overview/

Daniel.dosSantos@forescout.com
Simon.Guiot@forescout.com
Stanislav.Dashevskyi@forescout.com
Amine.Amri@forescout.com
Oussama.kerro@pwn-diaries.com