OT CYBERSECURITY

THE 2023 YEAR IN REVIEW

VULNERABILITY BRIEFING

Logan Carpenter
Vulnerability Analyst

Nick Cano
Vulnerability Analyst

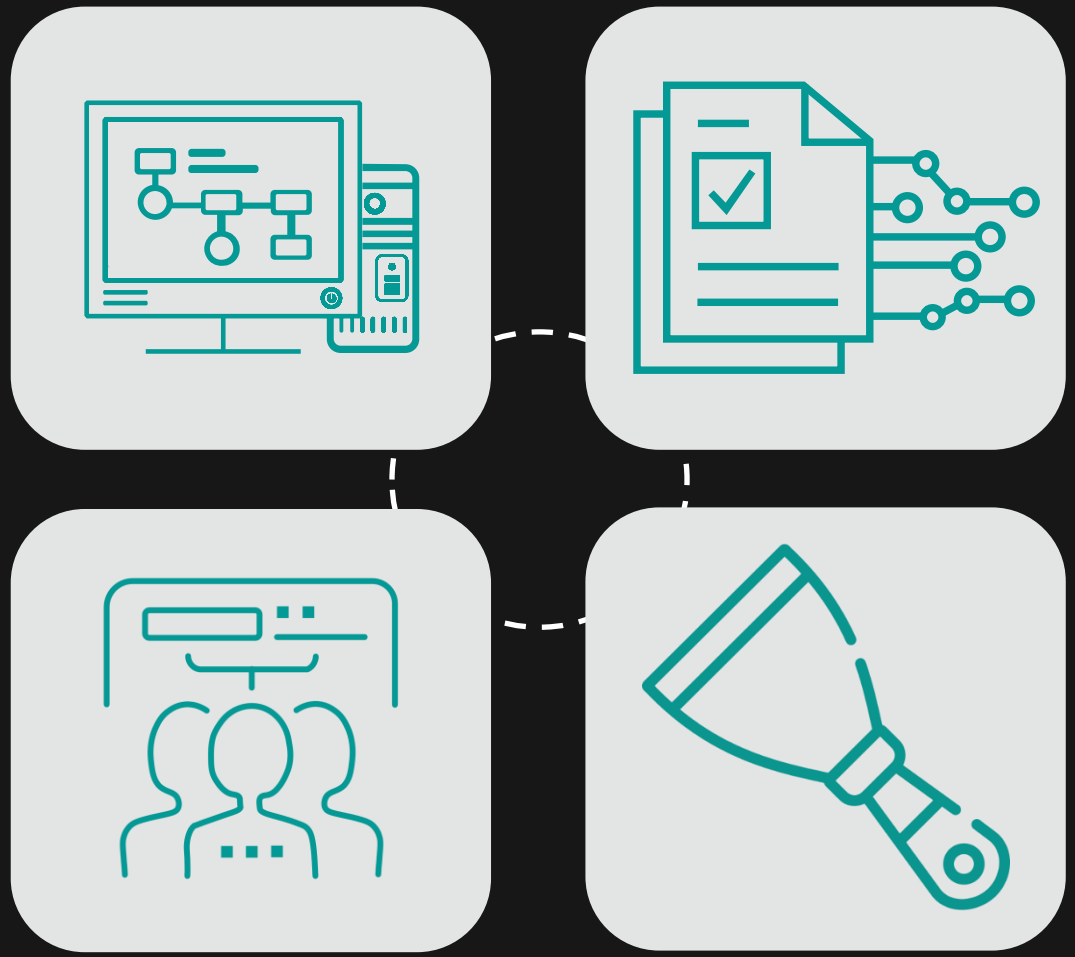
AGENDA

1. DRAGOS VULNERABILITY PROCESS
2. WHAT HAPPENED IN 2023?
3. NOTEWORTHY COMMON WEAKNESSES
4. PRIORITIZE NOW, NEXT, NEVER
5. FOCUS & FUTURE OUTLOOK
6. Q&A

Vulnerability Analysis Process & Impact

OBTAINING NEW VULNERABILITY DATA

Vendors, Public PSIRT Programs, Dragos Research, Government Advisories



Independent Researchers, Research Team/Companies, POCs

OT-CERT

In-House Scraper

VULNERABILITY ANALYSIS PROCESS

What is it?

Why does it matter?

What can we do about it?

- ✓ Assess individual CVEs
- ✓ Alternatives to patching
- ✓ CVSS corrections & prioritization
- ✓ OT-specific impacts

NOW

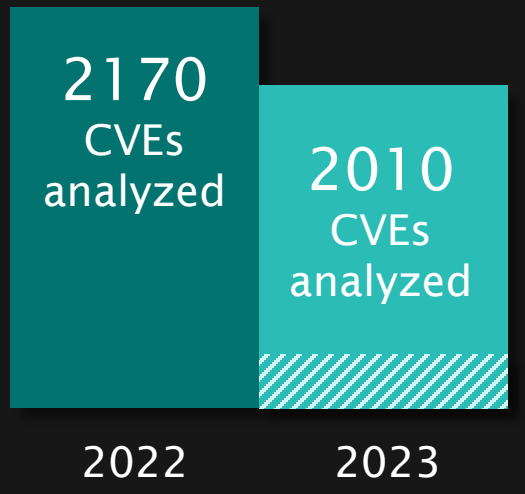
NEXT

NEVER

Vulnerability Stats 2023

HIGH-LEVEL OVERVIEW OF 2023

31% had incorrect CVSS data



14% had incorrect numeric scores, vectors, or both

Dragos provided missing mitigation advice for

49% of advisories

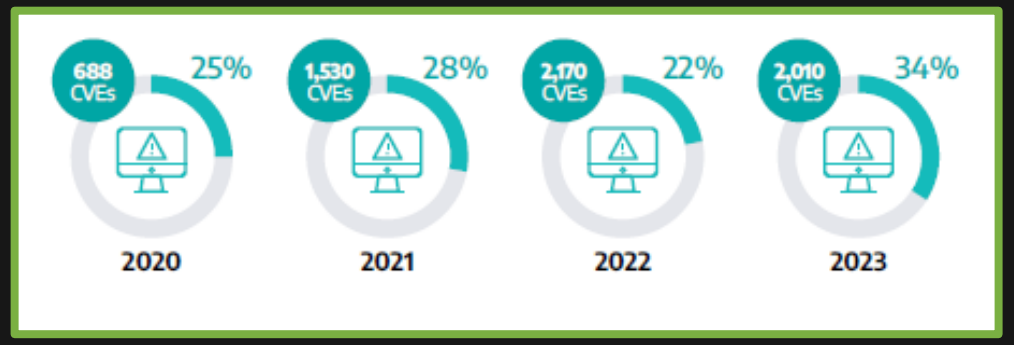
9% MORE SEVERE

4% less severe

1% were the same

RISE OF AUTHENTICATION REQUIRED VULNERABILITIES

VULNERABILITIES REQUIRING AUTHENTICATION TO EXPLOIT INCREASED ?



Potential reasons

- More Vendors are implementing authentication
- The low-hanging “No Auth” bugs have been mostly discovered.

Authentication does not equal secure

- Default credentials
- Backdoors
- Brute force / Credential theft

What Happened in 2023?

ROCKWELL AUTOMATION CONTROLLOGIX VULNERABILITIES

- US Gov disclosed vulnerabilities Rockwell Automation Devices after discovering zero-day vulns
- These issues were related to custom objects in Rockwell Automation CIP protocol
  - CVE-2023-3595 and CVE-2023-3596
- Rockwell Automation developed patches
- Multiple vendors were brought in to analyze vulns and detections

REAL TIME FEEDBACK FROM OT WATCH & NEIGHBORHOOD KEEPER

- Neighborhood Keeper participants and OT Watch Customers had visibility before the advisory went live
  - Allowed Dragos to identify issues with the provided detections and monitor for exploitation

TAKEAWAYS FROM OUR COLLABORATION

Neighborhood Keeper & OT Watch allow Dragos to quickly deploy analytics and IOCs for real-time feedback

Industry competitors can work together to safeguard civilization

Shoutout to Maggie Morganti from Rockwell Automation

HACKTIVIST ATTACKS ON UNITRONICS PLCs

In November 2023, CyberAv3ngers targeted Israeli-manufactured Unitronics PLCs

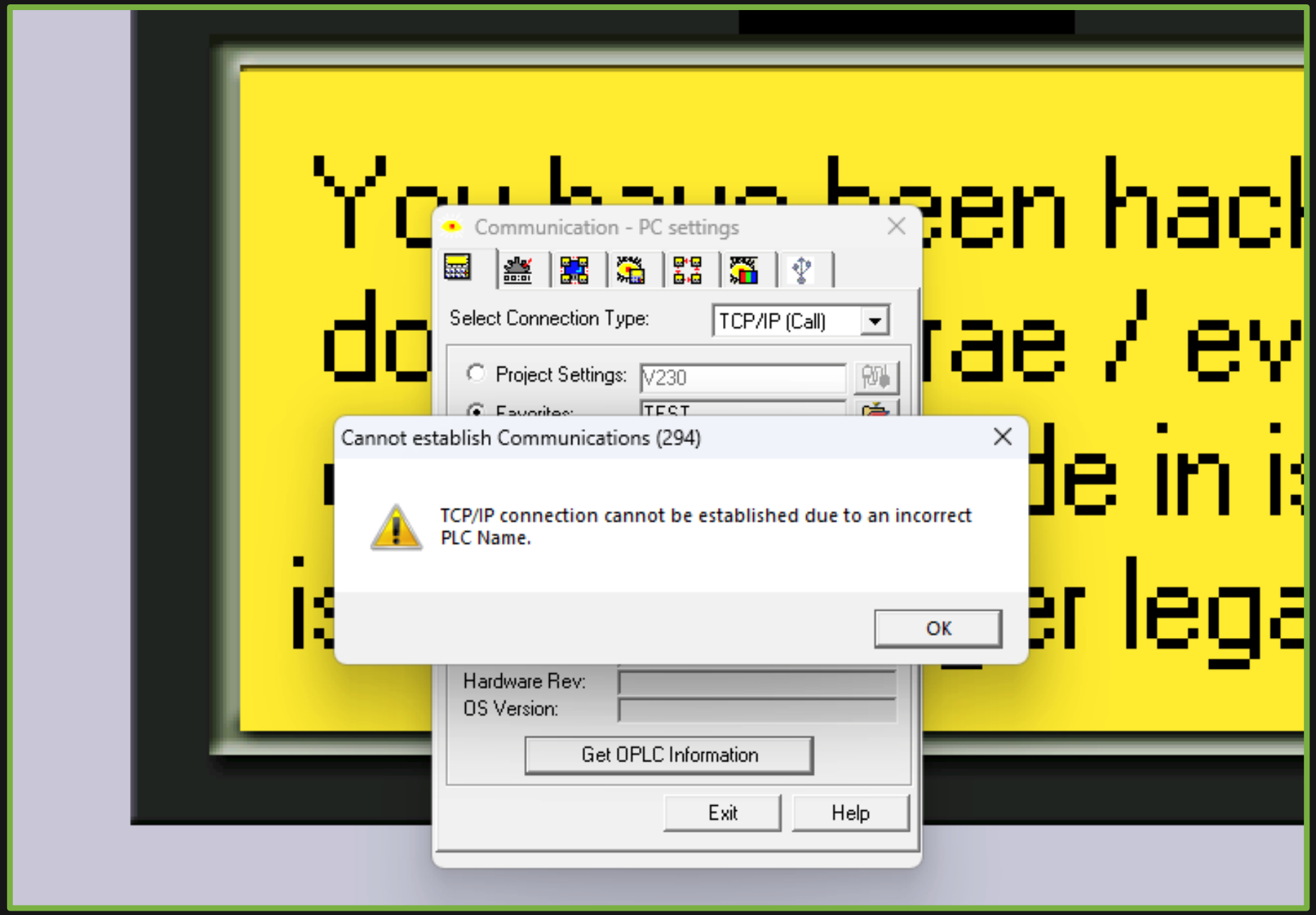
Targeted multiple sectors across the world

- Caused a local Water Scheme in North Ireland to go offline for two days
- Compromised a municipal water authority in Pittsylvania

Dragos analyzed a compromised PLC

UNITRONICS ROOT CAUSE

- Wiped ladder logic by sending blank ladder logic
  - This impacted operations
- Changed the PLCs name to #Gaza
  - Prevented the PLC management software from being able to connect to the PLC
  - You must know the PLC name to connect to the PLC
- Dragos assessed the password protection mechanisms
  - Three of the four available fail to prevent this type of attack
  - Password is retrievable


Communication - PC settings
Select Connection Type:
TCP/IP (Call)
Project Settings:
V230
Cannot establish Communications (294)
TCP/IP connection cannot be established due to an incorrect PLC Name.
OK
Hardware Rev:
OS Version:
Get OPLC Information
Exit
Help

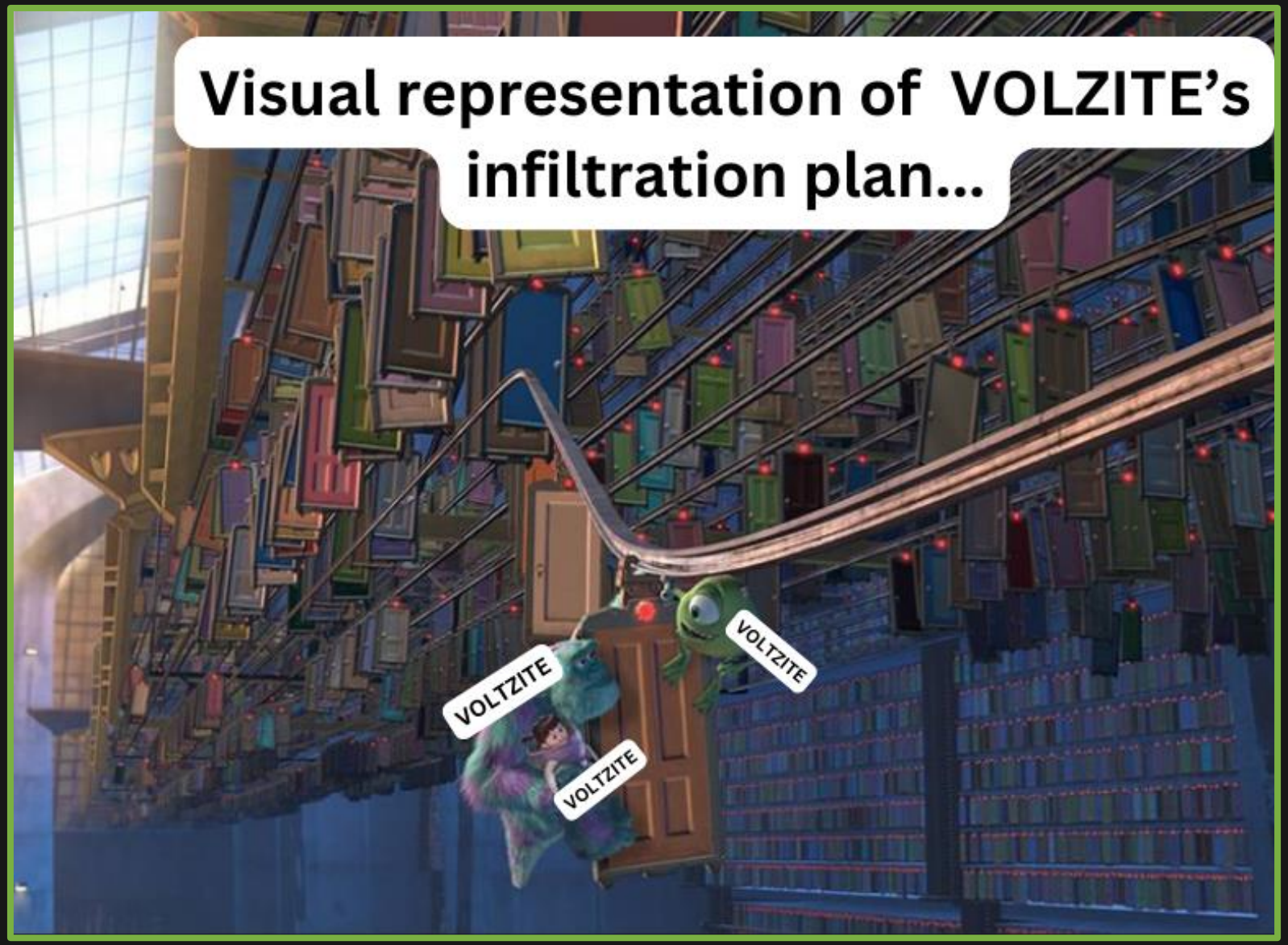
WHY THE ATTACKS ON UNITRONICS DEVICES MATTER?

THE PUBLIC GUIDANCE DOES NOT PREVENT EXPLOITATION

- There are still lots of unpatched devices connected to the internet
- CyberAv3ngers are still active and targeting vulnerable perimeter devices
- Dragos is still tracking their activity

VOLTZITE IVANTI ZERO-DAYS

- Abused by VOLTZITE aka Volt Typhoon
- Targets Ivanti Connect Secure VPN aka Pulse Secure
- CVE-2023-46805
  - Bypasses authentication
- CVE-2024-21887
  - Command injection vulnerabilities
  - Impacts multiple webserver endpoints
- Lots of implants, Lots of backdoors....


Visual representation of VOLZITE's infiltration plan...
VOLTZITE
VOLTZITE
VOLTZITE

Noteworthy CWEs

CWE VS CVE

This is the mistake.

CWE-20: Improper Input Validation

This is the vulnerability caused by the mistake.

CWE VS CVE

This is the mistake.

CWE-20: Improper Input Validation

This is the vulnerability caused by the mistake.

CWE-787/CWE-125: OUT-OF-BOUND READ/WRITE

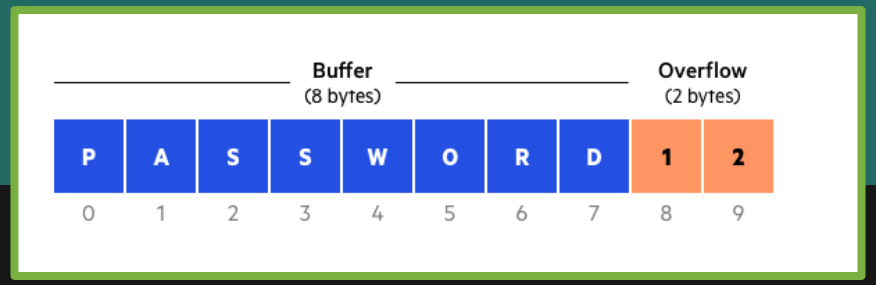
The most common CWE of last year

16% of all CVES assessed

Led in active exploitation

Over 40% are network exploitable

78% of these CVEs require no authentication



CWE-78: OS COMMAND INJECTION

- Second most exploited CWE
- Average CVE score of 9.2
- The highest among CWEs with more than one CVE
- The occurrence of these vulnerabilities has doubled over the past year
- 90% are remotely exploitable

Now, Next, Never

VULNERABILITY MANAGEMENT – PRIORITIZATION

A SMALL FRACTION OF VULNERABILITIES NEED IMMEDIATE ACTION

3%

OF ICS/OT VULNERABILITIES NEEDED TO BE ADDRESSED

NOW

68%

are network exploitable but addressing these can wait until the next maintenance cycle

These need to be addressed

NEXT

Mitigate through network monitoring, segmentation & MFA

29%

pose a possible threat but rarely require action

They likely NEVER need to be addressed

NEVER

Monitor these for signs of exploitation

ADDRESSING VULNERABILITIES NOW, NEXT, NEVER

NOW

- Actively exploited, public PoCs, disrupts OT environments
- Look into this right away

NEXT

- Network exploitable, but can be mitigated through network segmentation
- Look into this next and if there is time and resources

NEVER

- Complicated to exploit, require physical access, no impact to the OT environment
- No actions required, likely a waste of time

Focus Topics

FOCUS TOPIC: BUILDING TRUST WITH PRODUCT VENDORS

Understanding Sensitivity

- Vulnerability details can be sensitive.

Final Review

- Giving vendors final review of public content.

Perspective

- A Vulnerability is not the "end of the world.“

No fear Dragos is here

FOCUS TOPIC: PRODUCT VENDOR WINS!

Rockwell Automation

- Cross-vendor collaboration to get ahead of the adversary

Omron

- Very open-minded, responsive, and helpful in disclosing vulnerabilities that Dragos publicly disclosed

Phoenix Contact

- Dragos discovered vulns in their PLCNext runtime
- They sent Dragos newer loaner hardware to test our findings

Please, never hesitate to reach out!
intel@dragos.com

Nick Cano
Vulnerability Analyst

Logan Carpenter
Vulnerability analyst

Sam Hanson
Vulnerability Analyst

Kaysie Schippert
Vulnerability Analyst

Reid Wightman
Vulnerability Analyst

Kate Vajda
Director

Future Outlook

WHAT TO EXPECT IN 2024

- Deep dives by our Vulnerability team
- More IoT/IIOT assessments
- Windows and Cisco Vulnerability coverage in Platform
- S4 Presentation by Logan Carpenter will be public later this year

QUESTIONS AND ANSWERS

ENHANCE YOUR OT THREAT PREPAREDNESS.

Download the Report:
dragos.com/year-in-review