



Examining ICS Vulnerabilities

April 15th, 2021

WHAT IS THE YEAR IN REVIEW?

- Annual analysis of threats, vulnerabilities, assessments, insights
- Purpose is to help accelerate learning on how to address the challenges
- Fourth year running

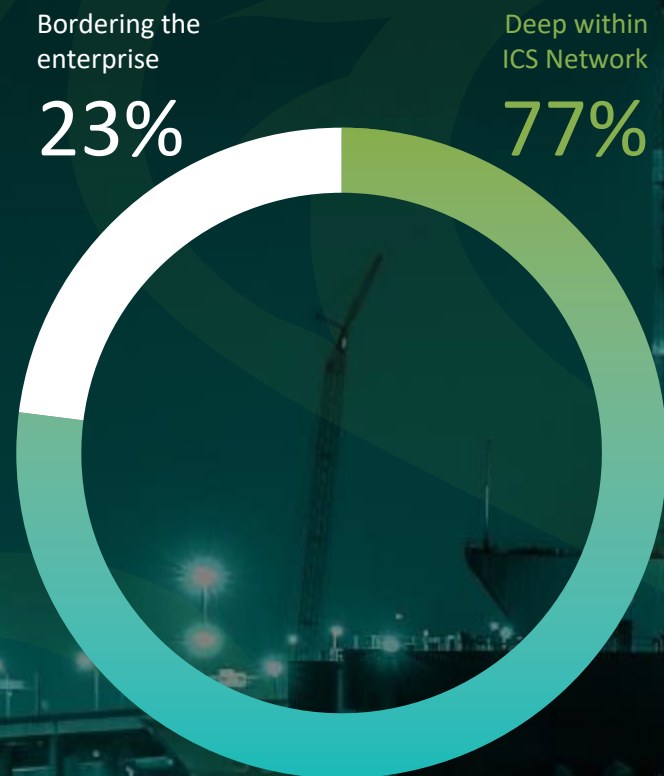


ABOUT THE DATASET

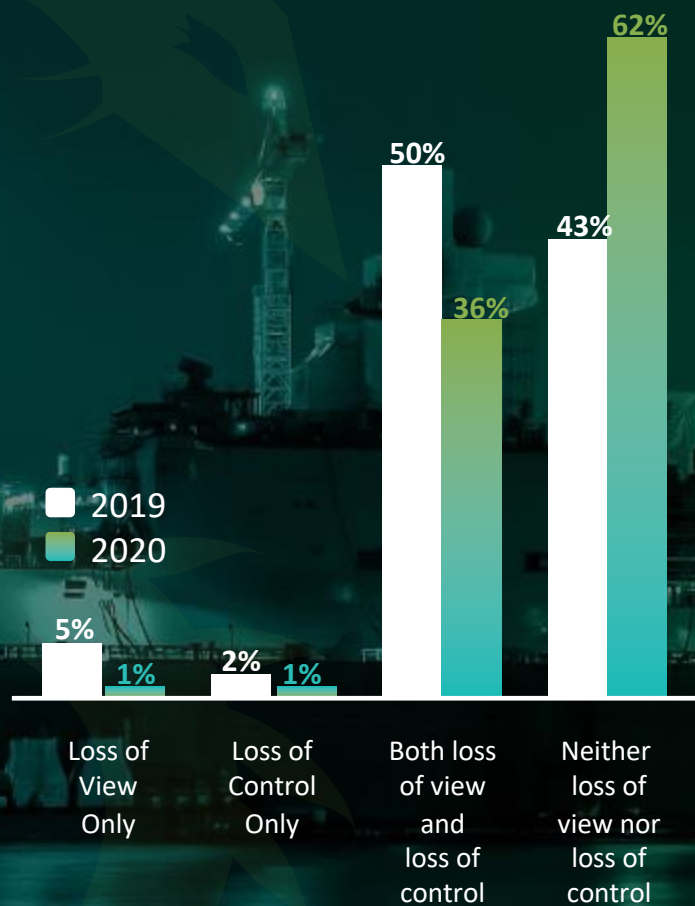
- 2020: 703 vulnerabilities / 253 advisories
- 2019: 438 vulnerabilities / 212 advisories
- Weekly review of new advisories, corrections and augmentation made. Updates as new data becomes available.

STATE OF ICS VULNERABILITIES

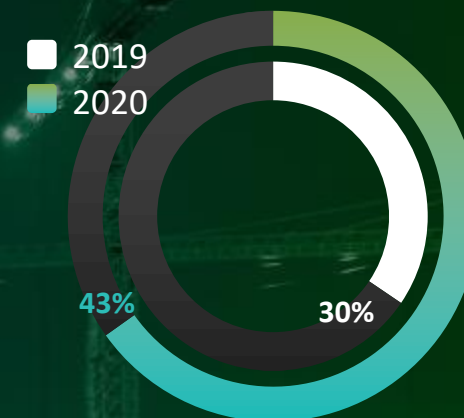
Where Vulnerabilities Reside



Impact of Disclosed Flaws



Advisories with Incorrect Data



Dragos Found to be LESS Severe than Public Advisory

26%

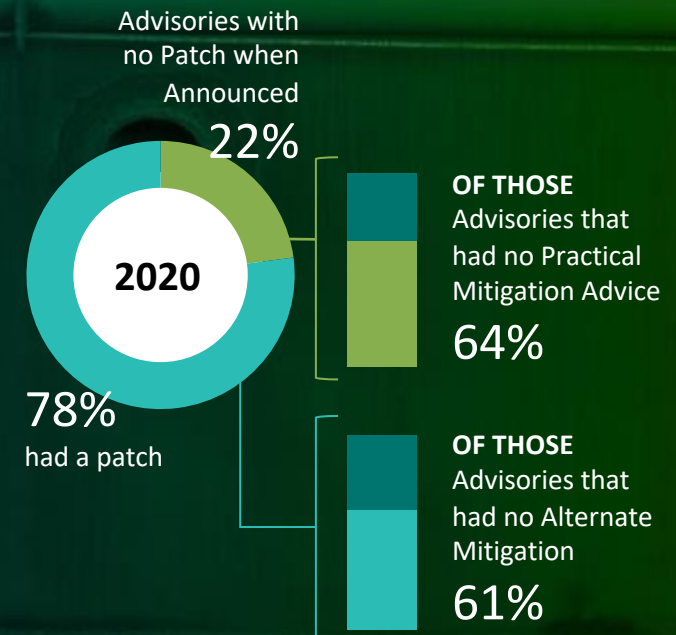
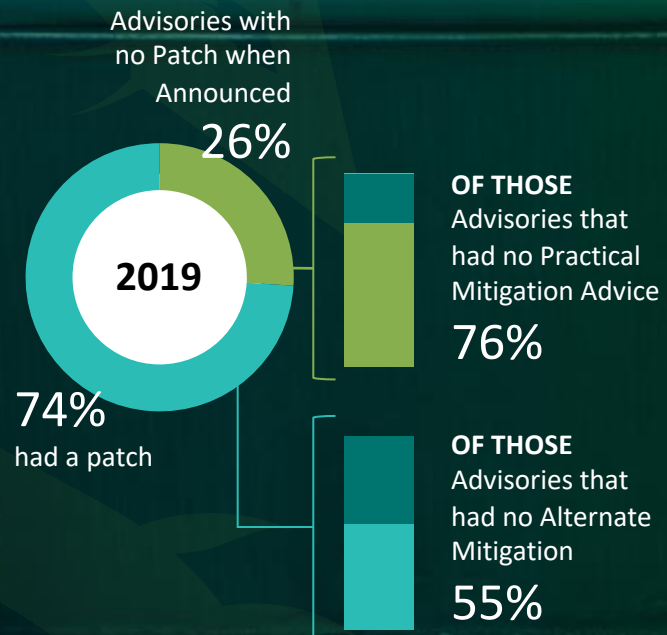
1% Identical Score but Different Exploitation Vector

Dragos Found to be MORE Severe than Public Advisory

73%

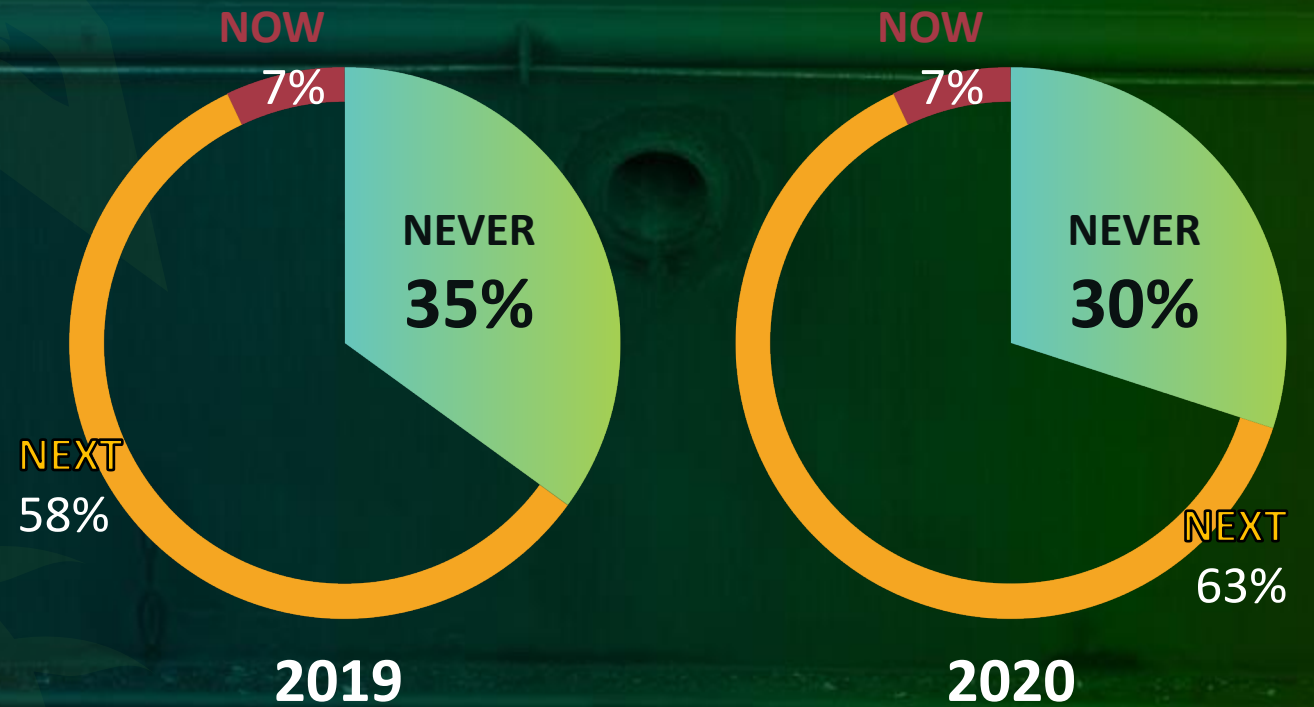
TAKING ACTION

Advisories Without Actionable Data



TAKING ACTION

NEVER, NEXT, NOW

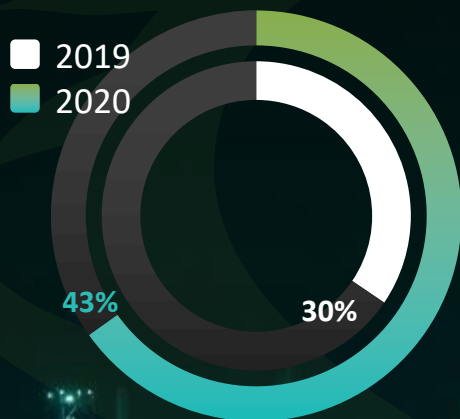


■ Never – Possible Threat/No Action ■ Next – Limited Threat ■ Now – Immediate Action

VULNERABILITIES

+ ICS CONTEXT FROM DRAGOS

Advisories with Incorrect Data



+ CVSS Score 5.3 >> 8.6

+ Mitigation advice

+ Operations Impact

Mitsubishi Electric MELSEC iQ-R series

09-June-2020

Immediate Action

The MELSEC series are programmable logic controllers deployed worldwide and commonly seen in the critical manufacturing industry.

Key Takeaways:

The MELSEC iQ-R series controllers are vulnerable resource exhaustion, which means that an attacker on the network can send a 2-byte payload to the device in order to crash the PLC.

To recover, the PLC would require a reboot, or possible a recalibration which could disrupt any production process. Restrict access to MELSEC devices (UDP/5006).

Note:

This advisory has been updated (Update B) in November, 2020 to include additional affected modules.

CVE-2020-13238 appears to have an incorrect CVSS. Dragos assesses that the score should be:


5.3 => 8.6

AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L => AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Mitsubishi Electric MELSEC iQ-R series Date: Jun 9, 2020 Source: ICS-CERT CVE-2020-13238 Dragos Assessment Restrict access to MELSEC devices (UDP/5006). Patch/Defense Details Upgrade to the latest patch, where available. Note, not all products currently have patches released.	Attributes Proof of Concept Exists No Active Exploitation No Skill Level Required Low Access Level Required Remotely Exploitable Physical Access Required Known Credentials User Interaction Security Impact Denial of Service Credential Exposure Code Execution/Modify App Broader Network Access Privilege Escalation Data Theft/Data Tamper Operation Impact Loss of View Loss of Control	Description Successful exploitation of this vulnerability could cause the Ethernet port to enter a denial-of-service condition. Affecting MELSEC iQ-R modules: R00/01/02CPU: Firmware Versions 7 or earlier R04/08/16/32/120CPU, R04/08/16/32/120ENCPU: Firmware Versions 39 or earlier R08/16/32/120SFCPU: Firmware Versions 20 or earlier R08/16/32/120PCPU: Firmware Versions 24 or earlier R08/16/32/120PSFCPU: Firmware Versions 05 or earlier RJ71EN71: Firmware Versions 49 or earlier Additional Resources ICSA-20-161-02
--	---	---

A BETTER WAY

Two most important questions to answer:

- What advisories are most important?
 - 8.6 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L)
or
 -  Immediate Action Required
- What action should be taken?
 - “Patch to version 6.9.12rc3”
or
 - “Restrict access to TCP/12601 if patching is not possible, ensure that only engineering workstations may access this service”

THE CALL

Vendors:

- Explain Industrial Impact
- Provide alternate mitigation advice

Researchers:

- Double-check those scores!
- Deep dive into industrial protocols, we need you.

End users/vuln triage:

- If upward advisory trend continues, may need to hire more!

Everybody:

Now/Next/Never

SPECIAL THANKS

The Rest of the Vuln Team: Kate Vajda, Jake Baines, Heyi Lu (Lu Lu)

Researchers that we bug with questions (you know who you are)

Vendors that are also willing to answer questions and provide clarity on underlying vulns

CONTACT US

Intel Team – intel@dragos.com

Sam Hanson: @SecureLoon (Twitter)

Reid Wightman: @ReverseICS (Twitter)

NEXT WEBINAR: APRIL 28



Asset Visibility in Action Using the Dragos Platform

Wednesday, April 28 at 1pm EDT

<http://dragos.com/asset-visibility-demo>