DRAGOS

VULNERABILITY BRIEFING

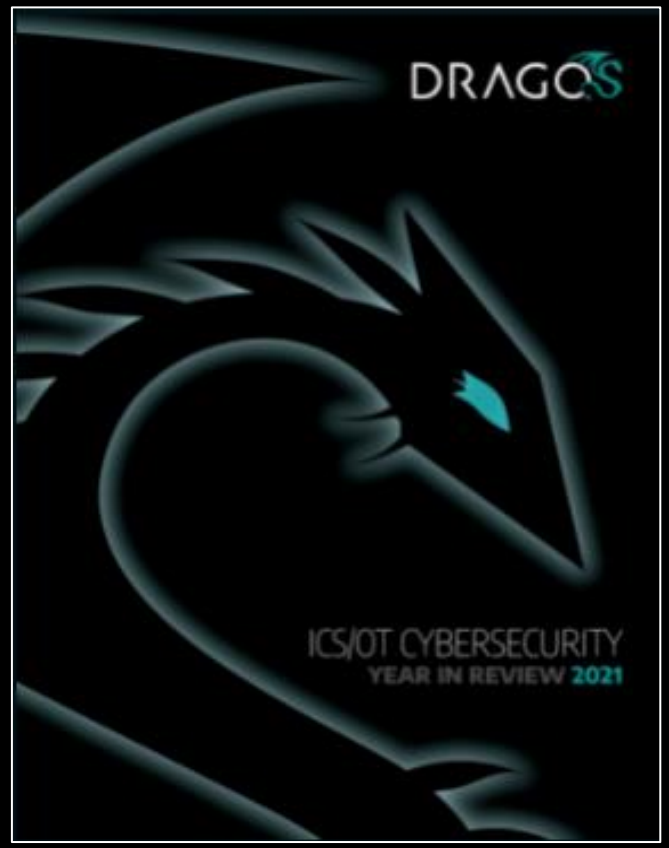
YEAR IN REVIEW 2021

Reid Wightman
Vulnerability Analyst
Dragos, Inc.

Sam Hanson
Vulnerability Analyst
Dragos, Inc.

What Is The Year In Review?

- Annual assessment and analysis of vulnerabilities
- Identify trends to help community manage risks and address challenges
- Fifth year running
- Tune into “Lessons Learned from the Frontlines” on 03/31 at 1pm EDT
- Ironically, vulnerability analysis started from a very different need…



2021: "A Year of Vulnerabilities"

Vulnerabilities made some major headlines
(for better or worse)

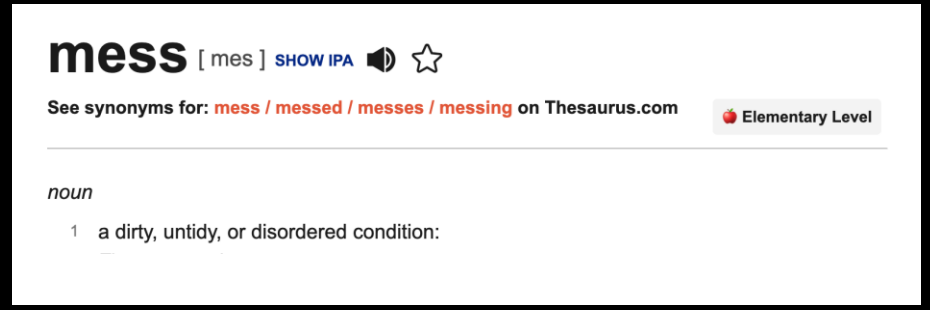
- Log4j
- PrintNightmare
- AMNESIA:33
- NAME:WRECK
- NUCLEUS:13
- Number:Jack
- INFRA:HALT
- BADALLOC
- ModiPWN

Log4j

CVE-2021-44228: RCE

CVE-2021-45046: RCE (non-default configurations)

CVE-2021-45105: Uncontrolled recursion leads to DoS



OPC FOUNDATION

jouniaro commented on Dec 13, 2021 — Contributor

Yes, we have been investigating CVE-2021-44228.

The OPC UA Java Stack itself is not directly vulnerable, since it is using the SLF4J for logging. So the issue depends on how the applications (such as the sample applications) then direct the SLF4J logging.

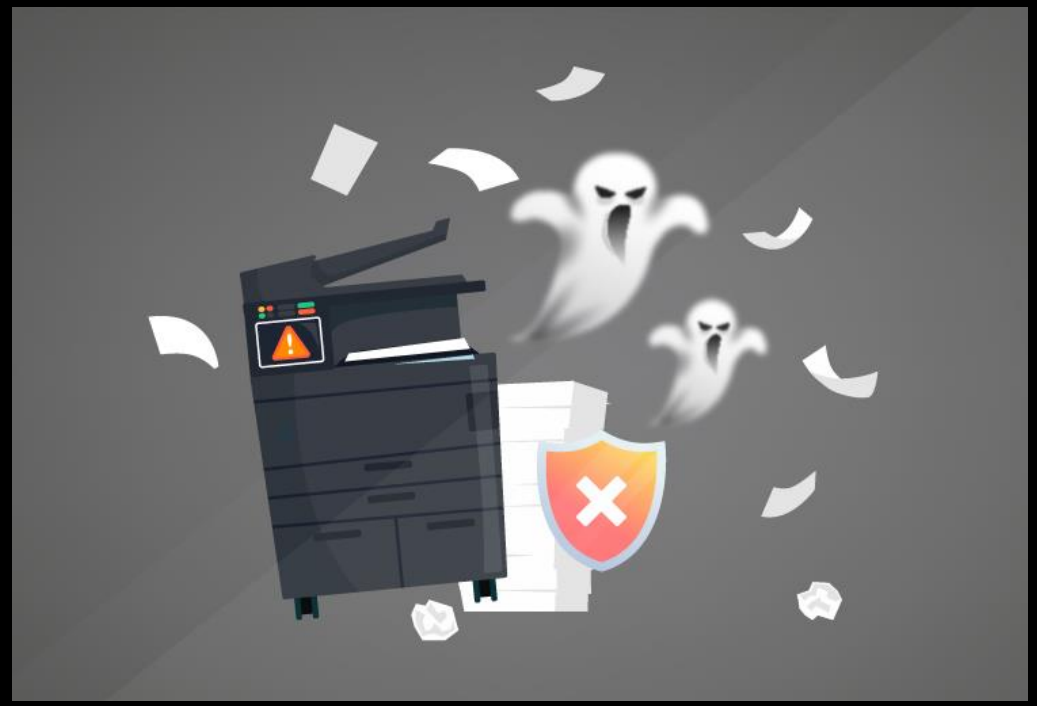
PrintNightmare

CVE-2021-34527: RCE

Enabled by default on Windows 7 SP1 - 10

Multiple Proof of Concepts available

May be leveraged to gain OT access via DMZ remote access workstations (jump boxes)



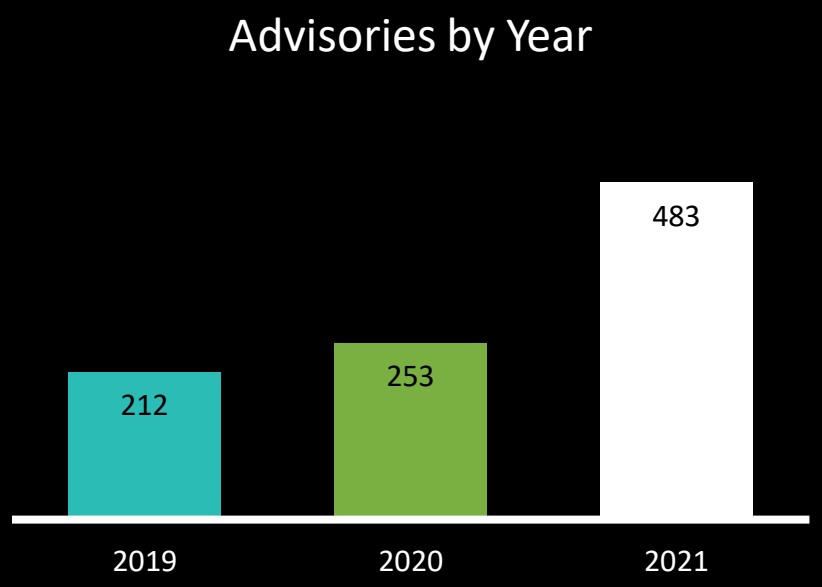
State of ICS Vulnerabilities

In 2021 there were:
More product advisories
More vulns (CVEs) per advisory
More high-severity vulns
More mistakes
When corrected, even more high-severity vulns

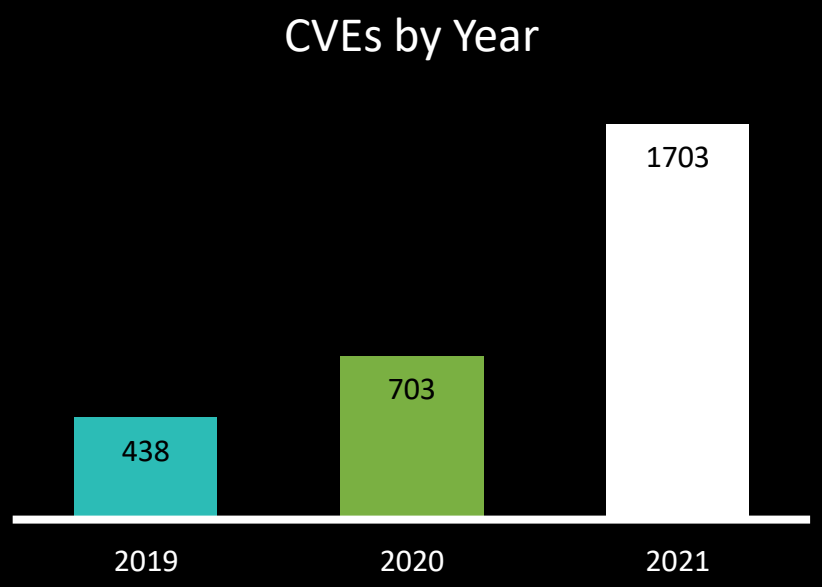
So let's talk:

How to better prioritize response
How to make response easier/faster

The Dataset

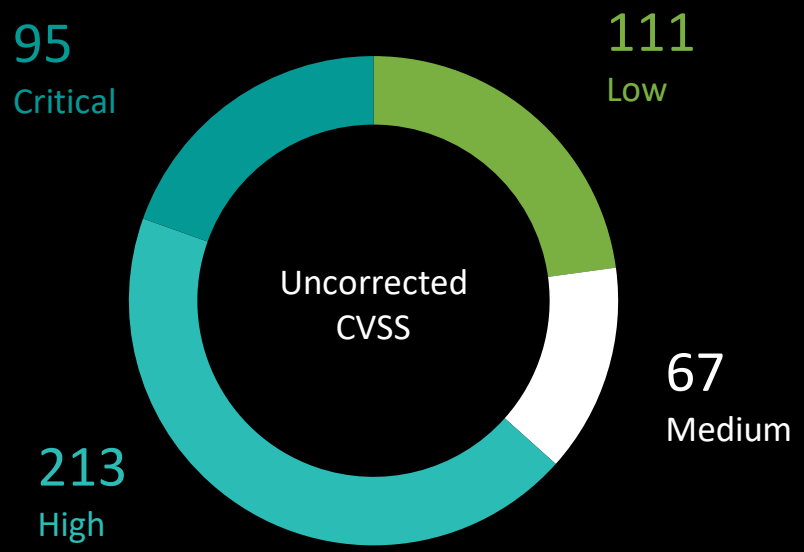


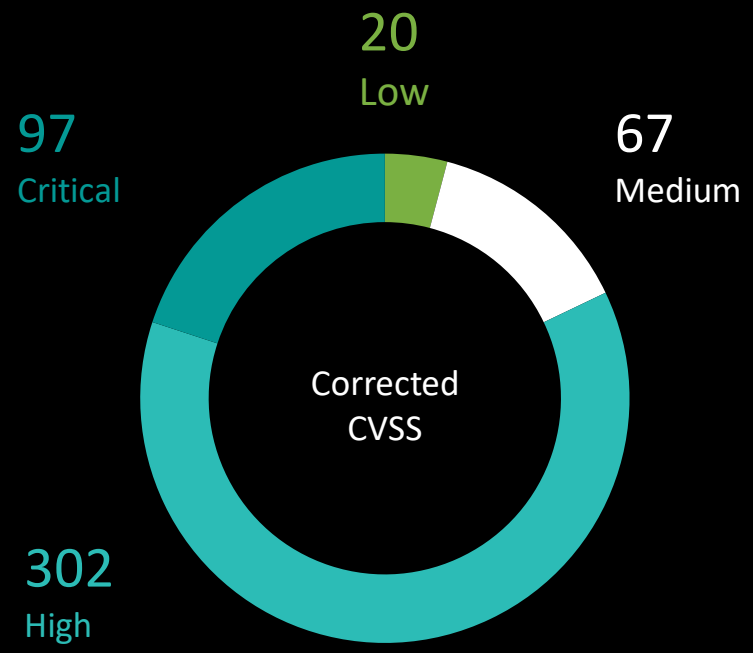
x1.9



x2.4

CVSS, Corrected CVSS, and Severity



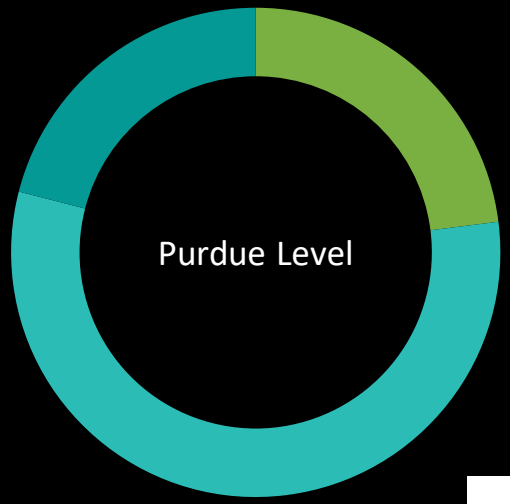


Frankly…

Where Do Vulnerabilities Reside?

Level 0 and 1

21%



Level 3.5, 4, and 5

23%

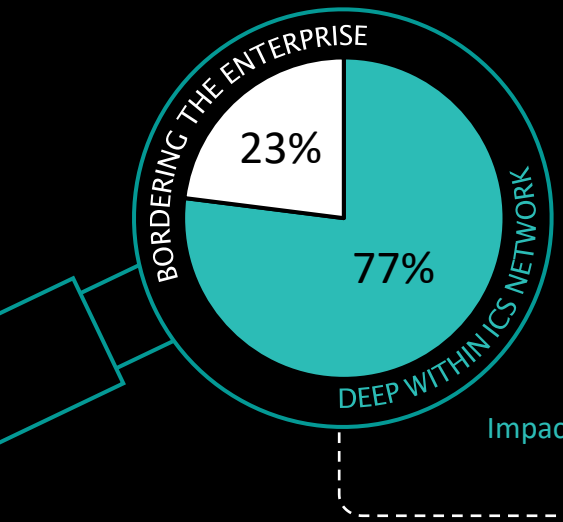
Level 2 and 3

56%

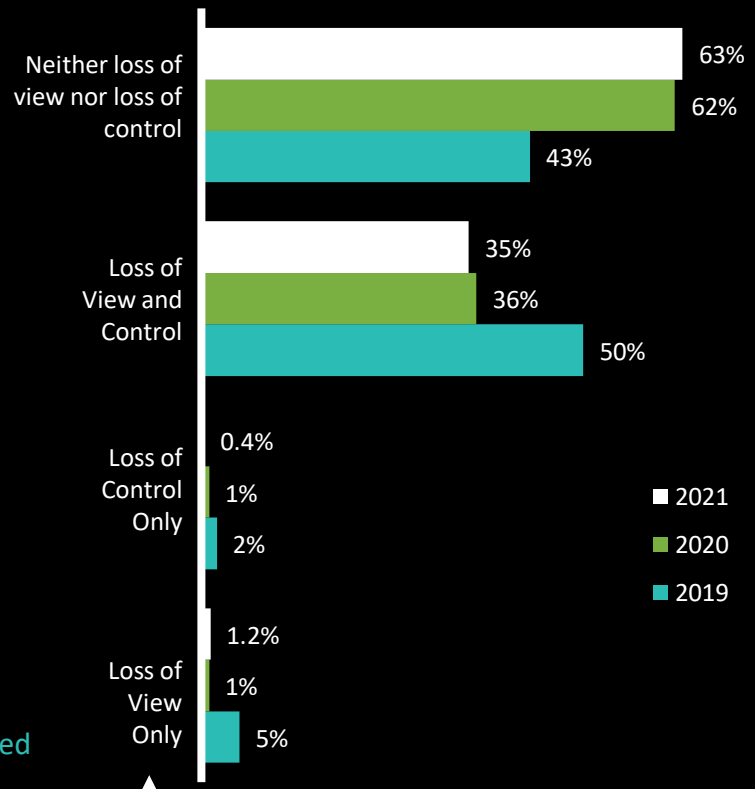
Better Priorization Through AI*

* Actual Intelligence

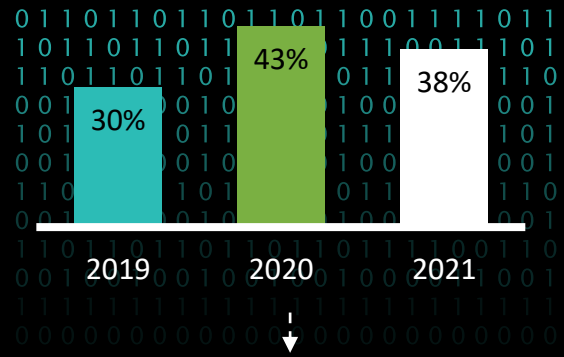
Where Vulnerabilities Reside



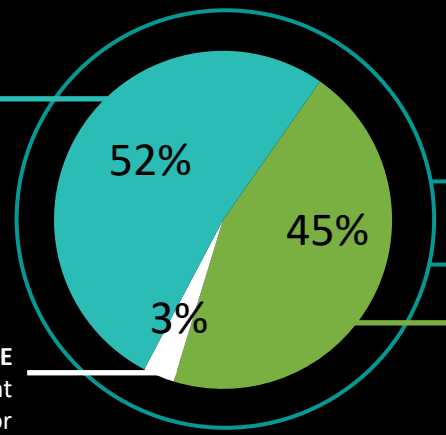
Impact of Disclosed Flaws



Advisories with Incorrect Data



Dragos Found to be **MORE SEVERE** than Public CVE data



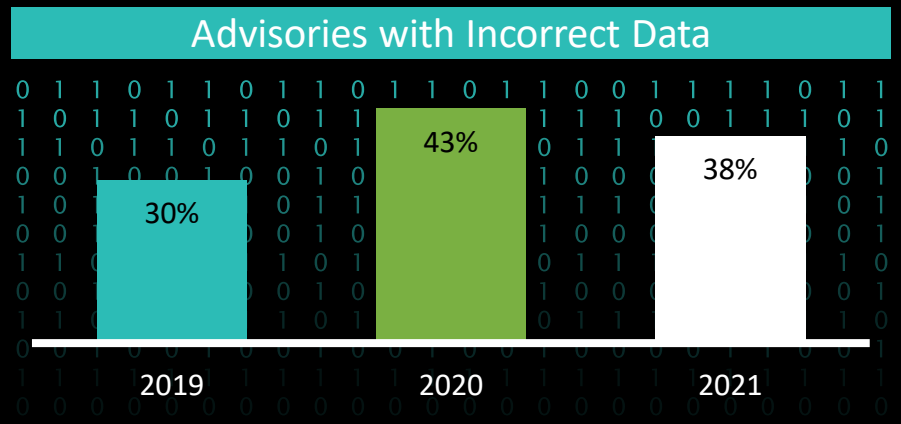
IDENTICAL SCORE but Different Exploitation Vector

Dragos Found to be **LESS SEVERE** than Public CVE data

Better Priorization Through AI*

* Actual Intelligence

+ ICS ENVIRONMENTAL CONTEXT FROM DRAGOS



Mitigation advice to restrict ports

CVSS Score 8 >> 8.8

Operations Impact

Emerson WirelessHART Gateway

05 October 2021

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action

Emerson WirelessHART Gateways provides access to instrumentation on a WirelessHART sensor network. The device queries instruments, and potentially actuators, for data, and presents this data for consumption by Human Machine Interfaces (HMIs), Instrument Management Systems (IMS), and other control system products including historians. They are deployed worldwide, most commonly in the Oil and Gas, Electric, Water and Wastewater Systems, Chemical, Critical Manufacturing, and Food and Agriculture industrial sectors.

Key Takeaways:

- There are vulnerabilities in Emerson WirelessHART Gateway that could allow an adversary to obtain and modify sensitive information, takeover user accounts, and execute code.
- An authenticated adversary could view and overwrite any file stored on the file system, modify system settings, takeover user accounts, obtain usernames and credentials, and inject Operating System (OS) commands and execute code.
- Restrict access to ports TCP/33333, TCP/5094, UDP/5094-5126. Enable the Remote Logging feature, found under System Settings -> Gateway -> Logging, to log messages to a remote syslog server. This can help identify tampering of the device and suspicious logons. Look for unexpected reboots, unexpected firmware upgrades/feature upgrades/system restoration in the log messages generated by the Gateway. Apply firmware security updates as soon as practically possible.

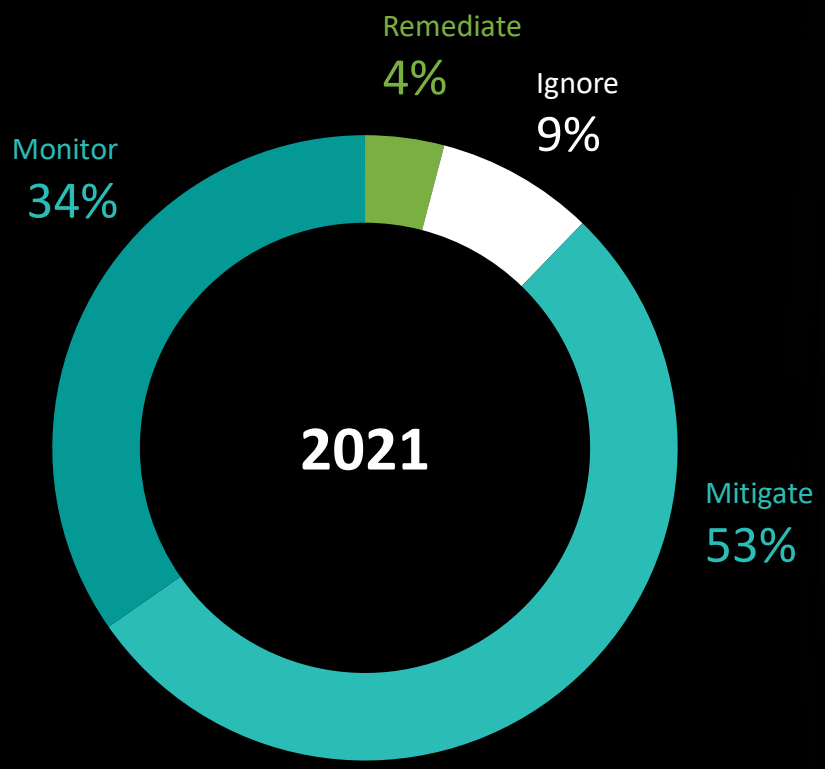
Note:

CVE-2021-24769 appears to have an incorrect CVSS. Dragos assesses that the score should be:

8 => **8.8**

Emerson WirelessHART Gateway	**Attributes**		**Description**
Date: Oct 5, 2021	Public Proof of Concept Exists	No	Successful exploitation could allow an authenticated adversary to view and overwrite any file stored on the file system, modify system settings, takeover user accounts, obtain usernames and credentials, and inject OS commands and execute code.
Source: ICS-CERT	Active Exploitation	No	
CVE-2021-85337	Skill Level Required	Low	**Affecting**
CVE-2021-03554	**Access Level Required**		• WirelessHART 1410 Gateway: prior to v4.7.94
CVE-2021-24769	Remotely Exploitable	✓	• WirelessHART 1410D Gateway: prior to v4.7.94
CVE-2021-22439	Physical Access Required		• WirelessHART 1420 Gateway: prior to v4.7.94
CVE-2021-81019	Known Credentials	✓	
CVE-2021-10073	User Interaction		**Additional Resources**
Dragos Assessment	**Security Impact**		Dragos Vulnerability Advisory: VA-2021-06
Restrict access to ports TCP/33333, TCP/5094, UDP/5094-5126. Enable the Remote Logging feature, found under System Settings -> Gateway -> Logging, to log messages to a remote syslog server. This can help identify tampering of the device and suspicious logons. Look for unexpected reboots, unexpected firmware upgrades/feature upgrades/system restoration in the log messages generated by the Gateway. Apply firmware security updates as soon as practically possible.	Denial of Service	✓	ICSA-21-278-02
	Credential Exposure	✓	
	Code Execution/Modify App	✓	
	Broader Network Access	✓	
	Privilege Escalation		
	Data Theft/Data Tamper	✓	
Patch/Defense Details	**Operation Impact**		
Update to a patched version, v4.7.94 or later.	Loss of View	✓	
	Loss of Control	✓	

Taking Action



Why We Hack Stuff

Some vulnerabilities just aren't worth it…

- A significant fraction of vulnerabilities are *not worth the time or risk to remediate*

ABB's PCM600 Engineering Tool

19-October-2021

Items of interest but likely requiring no action except in unique threat models

ABB's PCM600 is an engineering tool that provides functionality to manage and configure Relion protection and control IEDs through their lifecycle.

Key Takeaways:

- There is a vulnerability in the Update Manager Client of PCM600 that could allow an adversary to install software packages.
- An adversary could force the application to install potentially malicious software packages if they can trick an administrative user into kickstarting the installation process.
- Ensure installed software packages originate *only* from the URL *https://toolupdate.fi.abb.com/.* Ensure engineering workstations are not directly internet-facing.
- Dragos assesses with high confidence this vulnerability is unlikely to be used in a real world setting due to the requirements for successful exploitation.

Note:

CVE-2021-22278 appears to have an incorrect CVSS. Dragos assesses that the score should be:

6.7 => ***6.3***

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

ABB's PCM600 Engineering Tool

Date: Oct 19, 2021
Source: ABB
CVE-2021-22278

Dragos Assessment

Ensure installed software packages originate *only* from the URL *https://toolupdate.fi.abb.com/.* Ensure engineering workstations are not directly internet-facing.

Dragos assesses with high confidence this vulnerability is unlikely to be used in a real world setting due to the requirements for successful exploitation, namely since local access to the host and tricking an administrator into downloading a software package is required.

Patch/Defense Details

Update to a patched version of the PCM600 Update Manager, v2.4.21218.1 or later.

Attributes	
Public 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 could allow a locally authenticated adversary to force the application to install potentially malicious software packages if they can trick an administrative user into kickstarting the installation process.

Affecting

- PCM600 Update Manager Client: prior to v2.7 through v2.10

Additional Resources

ABB's Security Advisory

Corrections: In-Depth

Example 1: Missing information and no CVE assignment

Note:
CVEs have not been assigned for these issues. Dragos assesses the following CVSSv3 scores:

- Hard-coded Cryptographic Key in Firmware: 9.8 - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Hard-coded Cryptographic Key in Program Component: 7.5 - AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
- Use of Platform-dependent Third-party Components with Vulnerabilities: not enough information provided in the vendors security advisory to accurately assess the score of this vulnerability.

Example 2: CVE duplicates

Note:
ICS-CERT has incorrectly duplicated CVE-2020-5806. One of those duplicates should be CVE-2020-5807.

Note:
Some vulnerabilities in this advisory are duplicates:

- CVE-2021-22648 is a duplicate of CVE-2020-28988 and CVE-2020-28990.
- CVE-2021-22640 is a duplicate of CVE-2020-28987.

The original CVE's can be found in a past advisory.

Note:
Some vulnerabilities mentioned in the ICS-CERT advisory appear to be duplicates of previously discovered vulnerabilities by Dragos researchers.

- CVE-2021-85337, CVE-2021-22439, and CVE-2021-31527 seem to all be the same issue.
- CVE-2021-31526 also appears to be a duplicate of CVE-2021-24769.

Dragos researchers have reached out to Emerson to verify they are duplicates.

Corrections: In-Depth

Example 3: Incorrect CVSS scores

CVE-2021-22640 appears to have an incorrect CVSS. Dragos assesses that the score should be:
7.5 => ***5.9***
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N => AV:N/***AC:H***/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2021-22650 appears to have an incorrect CVSS. Dragos assesses that the score should be:
7.5 => ***9.8***
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N => AV:N/AC:L/PR:N/UI:N/S:U/C:H/***I:H***/***A:H***

Example 4: Vulnerability type misunderstandings

Note:
The ICS-CERT advisory for this vulnerability states that the issue requires no user interaction. Dragos assesses that the vulnerability is a file format issue and that a local user would have to open a corrupt project in order to exploit the issue.

Asset Identification–The CPE Problem

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

AND

OR

cpe:2.3:o:siemens:simatic_s7_1200_cpu_firmware:*:*:*:*:*:*:*:*	Up to (including)
Show Matching CPE(s)	4.1.2

OR

cpe:2.3:h:siemens:simatic_s7_1200_cpu:-:*:*:*:*:*:*:*

Show Matching CPE(s)

Configuration 7 (hide)

cpe:2.3:o:siemens:simatic_s7-1200_firmware:-:*:*:*:*:*:*:*

Show Matching CPE(s)

Running on/with

cpe:2.3:h:siemens:simatic_s7-1200:-:*:*:*:*:*:*:*

Show Matching CPE(s)

Known Affected Software Configurations Switch to CPE 2.2

Configuration 1 (hide)

cpe:2.3:o:siemens:simatic_s7-1200_cpu_firmware:4.5.0:*:*:*:*:*:*:*

Show Matching CPE(s)

Running on/with

cpe:2.3:h:siemens:cpu_1211c:-:*:*:*:*:*:*:*

Show Matching CPE(s)

cpe:2.3:h:siemens:cpu_1212c:-:*:*:*:*:*:*:*

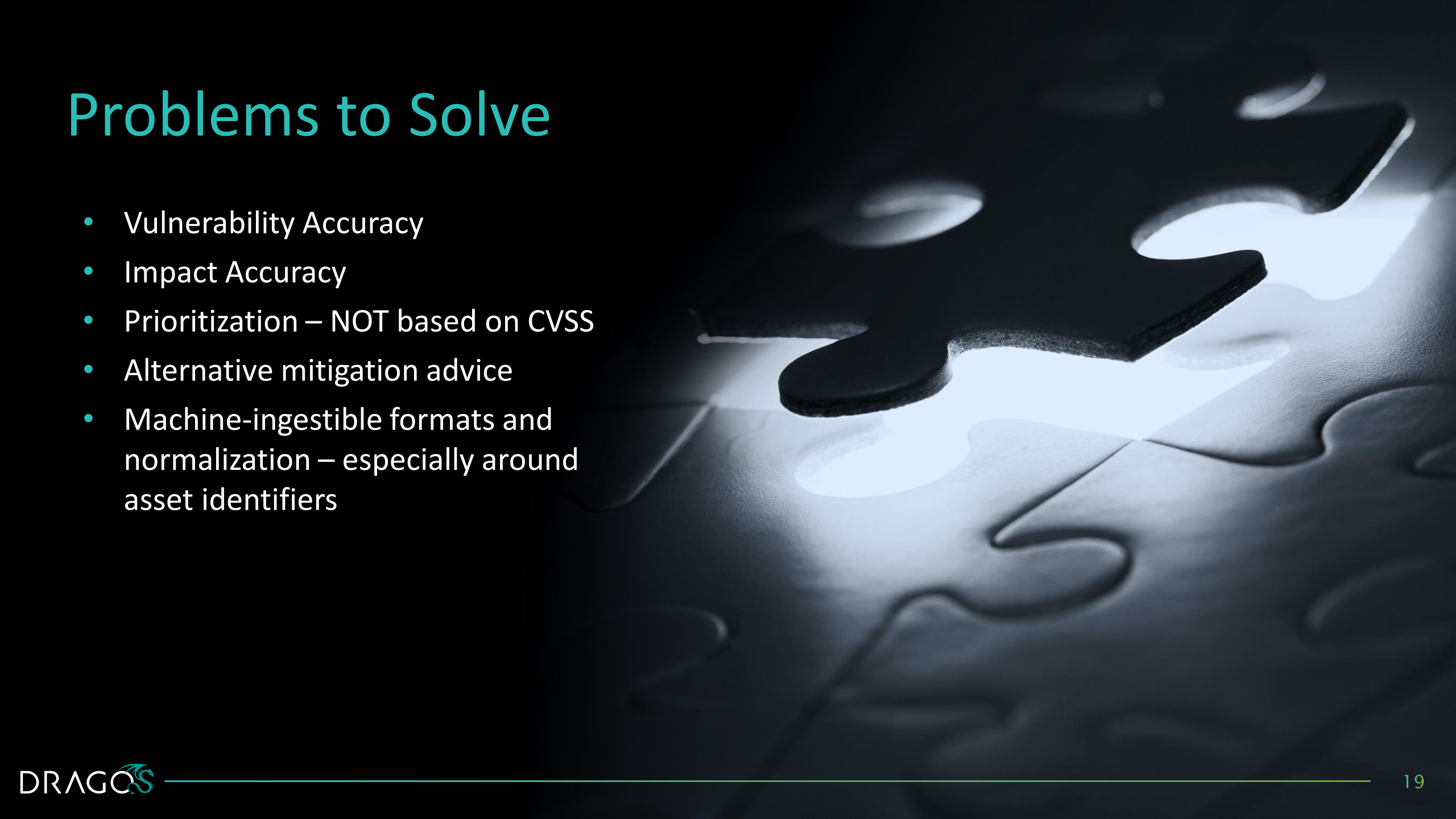
Show Matching CPE(s)

cpe:2.3:h:siemens:cpu_1212fc:-:*:*:*:*:*:*:*

Show Matching CPE(s)

Problems to Solve

- Vulnerability Accuracy
- Impact Accuracy
- Prioritization – NOT based on CVSS
- Alternative mitigation advice
- Machine-ingestible formats and normalization – especially around asset identifiers



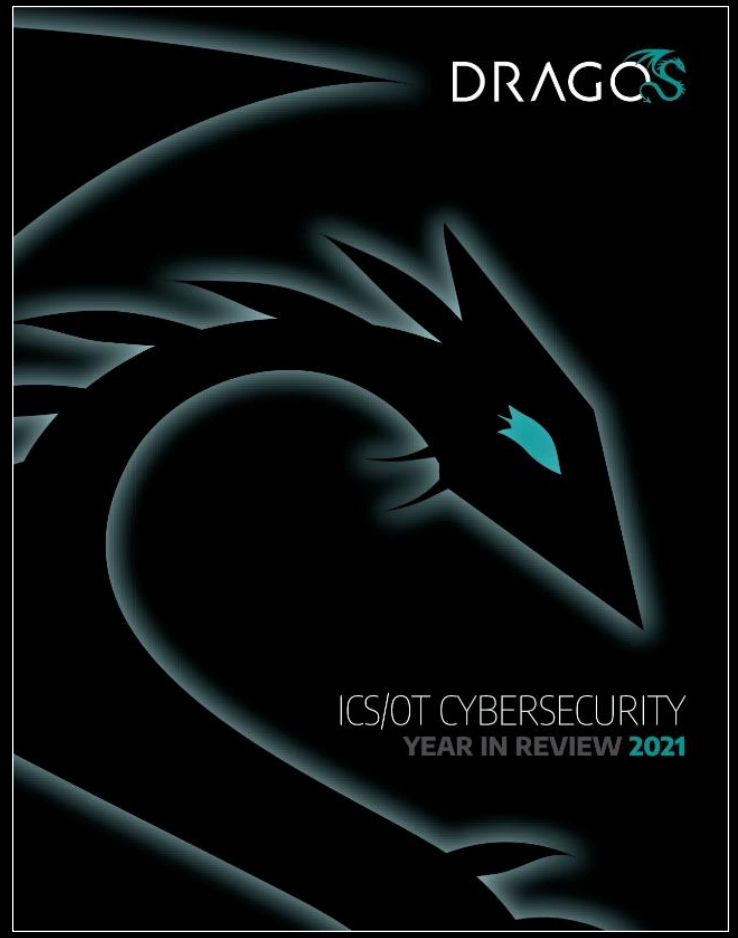
QUESTIONS AND ANSWERS

Thank You

Reach out Intel Team at intel@dragos.com

Reid Wightman
Vulnerability Analyst
e: rwightman@dragos.com
t: @reverseics

Sam Hanson
Vulnerability Analyst
e: shanson@dragos.com
t: @secureloon



To download a copy of the
2021 Year In Review Report,
Visit: dragos.com/yir