




Whitepaper

EXAMINING ICS/OT EXPLOITS: FINDINGS FROM MORE THAN A DECADE OF DATA

Jacob Baines

Principal Industrial Control Vulnerability Analyst
Threat Intelligence | Dragos, Inc.

 info@dragos.com


 [@DragosInc](https://twitter.com/DragosInc)

TABLE OF CONTENTS

Executive Summary 3

 Key Findings..... 4

Public ICS/OT Exploit Defined 5

About The Data Set..... 6

Public ICS/OT Exploits..... 7

 Why Care About Public ICS/OT Exploits At All? 7

 Publication Trends..... 8

 Affected Vendors 12

 Viewed Through The Purdue Model..... 13

 Impactful Exploits 15

 Mostly Useless 17

 Author Affiliation 18

 Time To First Public Exploit..... 21

 In The Wild 23

Conclusion 24

References 25

EXECUTIVE SUMMARY

Dragos currently tracks¹ more than 3000 CVEs (Common Vulnerabilities and Exposures) published since 2010 that affect Industrial Control Systems and Operational Technology (ICS/OT) networks. Of these CVEs, more than 400 have publicly available exploits.

Some have multiple public exploits, resulting in Dragos tracking nearly 600 public ICS/OT exploits. **Public exploits significantly lower the skill and effort needed to exploit a vulnerability.** The public exploits tracked by Dragos affect every level of an industrial environment as described in the Purdue Model², providing adversaries pre-packaged tools that are capable of infiltrating and spreading through an ICS network. Adversarial usage of public exploits on ICS networks is not theoretical. Dragos tracks multiple Activity Groups (AG) that use public exploits.

The public ICS/OT exploits tracked by Dragos have been developed by hundreds of individuals. They affect products developed by more than a hundred vendors, and their impact on the industrial process runs the gamut. Leveraging the knowledge of these exploits and then using the guidance in this paper will help ICS operators better determine which vulnerabilities to remediate.

KEY FINDINGS

- > **HIGHLY IMPACTFUL PUBLIC ICS/OT EXPLOITS AFFECT** every level of industrial environments (i.e., every Purdue Level).
- > **THIRD-PARTY RESEARCH ADVISORIES ARE THE MOST** prevalent public exploit source.
- > **THE TIME TO FIRST PUBLIC EXPLOIT IS TYPICALLY WITHIN** 30 days of public disclosure.
- > **10% OF THE PUBLIC ICS/OT EXPLOITS ARE KNOWN TO HAVE** been used in the wild. Dragos estimates this number is low and will increase as visibility into ICS/OT networks improves.
- > **NEARLY 50% OF ALL PUBLIC ICS/OT EXPLOITS ORIGINATED** from researchers at a company or university.
- > **A HANDFUL OF WELL-KNOWN ORGANIZATIONS PUBLISH** nearly 25% of all public exploits.
- > **BOTH THE AMOUNT OF ICS/OT EXPLOITS AND THE** percentage of ICS/OT CVEs with a public exploit dropped in 2020. These datapoints may indicate that fewer vulnerability researchers are publishing exploits at disclosure time.
- > **THE ABILITY TO PIVOT AND PERSIST WITHIN AN ICS** network is the the most common impact of a public ICS/OT exploit.
- > **ALMOST 30% OF ICS/OT PUBLIC EXPLOITS HAVE** requirements like user interaction, man in the middle positioning, or non-default configurations, that make them potentially useless within the context of an ICS/OT network.
- > **VULNERABILITY REMEDIATION SHOULD FOCUS MOSTLY ON** those vulnerabilities that have a public proof of concept and a low attack complexity, starting with those known to exploit ICS environments.

PUBLIC ICS/OT EXPLOIT DEFINED

An **exploit** is a tool that allows an adversary to bypass a security boundary within a piece of software or hardware. Exploits come in many forms. An exploit can be a curl command³, a URI⁴, a blob of HTTP data⁵, or even a reasonably written description⁶. Dragos considers anything that allows a low skilled adversary to knowingly and quickly bypass a security boundary to be an exploit.

While our interpretation of what constitutes an exploit is fairly liberal, the exploits in our data set are typically represented in code.

Exploit Medium

For Vulnerabilities Published From 2010 to Early 2021

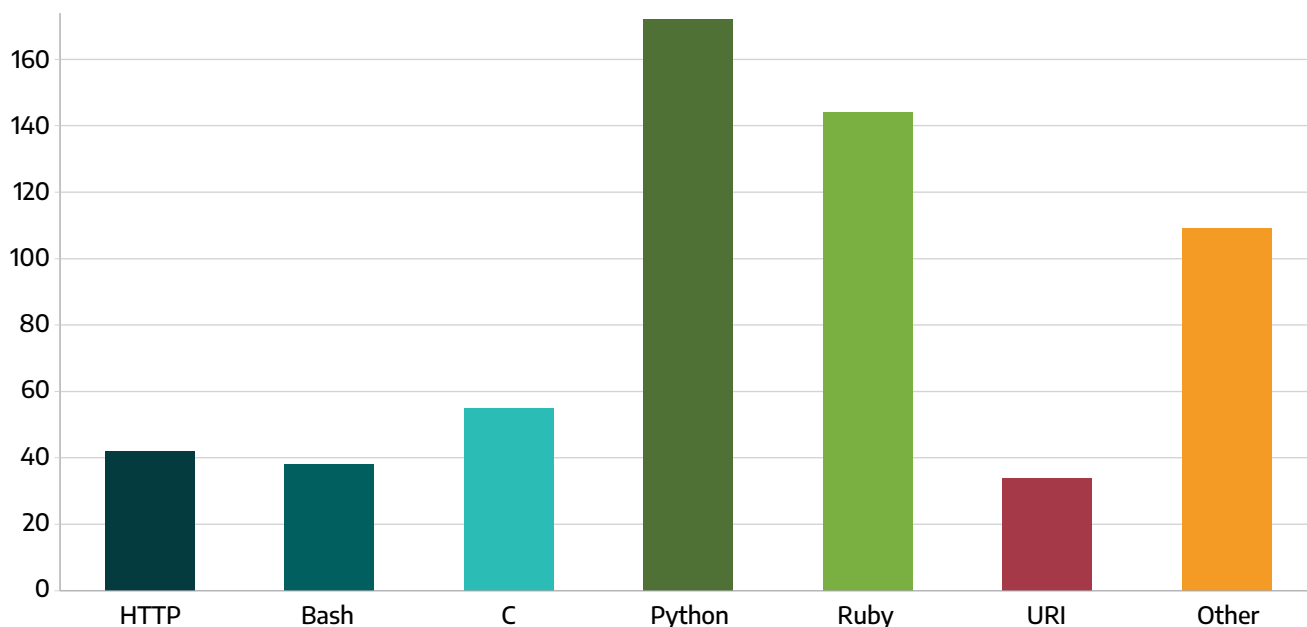


Figure 1: Exploit Mediums for public ICS/OT vulnerabilities from 2010 to early 2021.

The **Other** category in **Figure 1** is comprised of a smattering of other mediums such as wget⁷, HTML, netcat⁸, openssl⁹, and just about every programming language under the sun.

An exploit is considered “public” when it is freely available to anyone. For example, exploits posted to Exploit Database¹⁰ (Exploit-DB) are considered public because there are no restrictions to accessing Exploit-DB. Exploits that are part of for-purchase frameworks like CANVAS¹¹ are not considered public. Exploits that are only shared amongst security researchers are not considered public. Exploits only found on the dark web are not considered public as they require special methods to access them. Generally speaking, an exploit is treated as public if it is accessible by simply visiting a link.

An exploit is considered ICS/OT-related when it can reasonably be determined to affect a system within an ICS/OT network. For some systems it is obvious. PLCs, HMIs, and Historians are ICS/OT-related. Likewise, products developed by Rockwell and Schneider Electric are likely to be ICS/OT-related.

There are a lot of less obvious ICS/OT-related systems though. For example, Dragos customers have VPN appliances in their ICS networks and ICS-specific activity groups like PARISITE¹² target them for Stage 1, initial access¹³. Similarly, Dragos's experience and the Oldsmar Water Treatment Facility incident¹⁴ show that remote desktop solutions are deployed in ICS networks. While VPN appliances and remote desktop solutions are not ICS-specific, it is reasonable to describe

these systems as ICS/OT-related.

Perhaps more controversial is how to handle Microsoft Windows Operating System (Windows OS) exploits. Many ICS/OT systems are deployed on top of Windows, and exploits like ETERNALBLUE¹⁵ (MS17-010¹⁶) have been used to infiltrate ICS/OT networks on a number of occasions¹⁷. We therefore include it in our data set even though it isn't an ICS/OT vulnerability per se. But not all Windows vulnerabilities are practical within an ICS/OT network. Currently, the only public Windows OS exploits included in our data set are unauthenticated, remote exploits affecting default services or services we deem reasonable to be present in an ICS network (for example, Remote Desktop).

ABOUT THE DATA SET

This paper covers vulnerabilities published between 2010 and April 2021. Vulnerability publication can refer to a National Vulnerability Database¹⁷ (NVD) entry, a vendor advisory, a researcher advisory, or a third-party advisory such as those produced by Industrial Control Systems Computer Emergency Response Team¹⁸ (ICS-CERT). The contents of the CVEs in the data set are not restricted to CVEs issued from 2010 onwards. For example, an ICS-CERT advisory published in 2015¹⁹ indicated that a Honeywell product was vulnerable to CVE-2007-6483²⁰. Although CVE-2007-6483 was originally published in 2007, the 2015 advisory proved it remained relevant to our 2010 to April 2021 timeline. As such, CVE-2007-6483 and the corresponding public exploit²¹ are included in our data set.

The data set relies on some self-reported information. Where possible, we use

official data such as that published by NVD or ICS-CERT. However, much of the data set is gleaned from personal blogs, researcher advisories, and scraps of code shared on the internet. Our approach was to trust the data as presented. For example, if the exploit indicates the author works for Rapid7, we trust that is true. If we happen to know an individual works for a specific company, but they do not include that association in their exploit then we do not include it in our data either. For example, the user LiquidWorm²² on Exploit-DB is a well-known vulnerability researcher that sometimes publishes exploits related to their day job under the LiquidWorm handle. However, the exploits are typically not labeled as such. In our data, those exploits are treated as if they were developed by an "unaffiliated" author. While imperfect, this ensures we are not introducing our own biases or mistakes into the data.

The data set also uses the *NVD Published Date* timestamp to mark publication of CVE. This is not entirely accurate, as NVD publication can lag behind the actual disclosure date. The lag time is typically measured in days.

It should also be understood that there is a non-measurable amount of bias within the

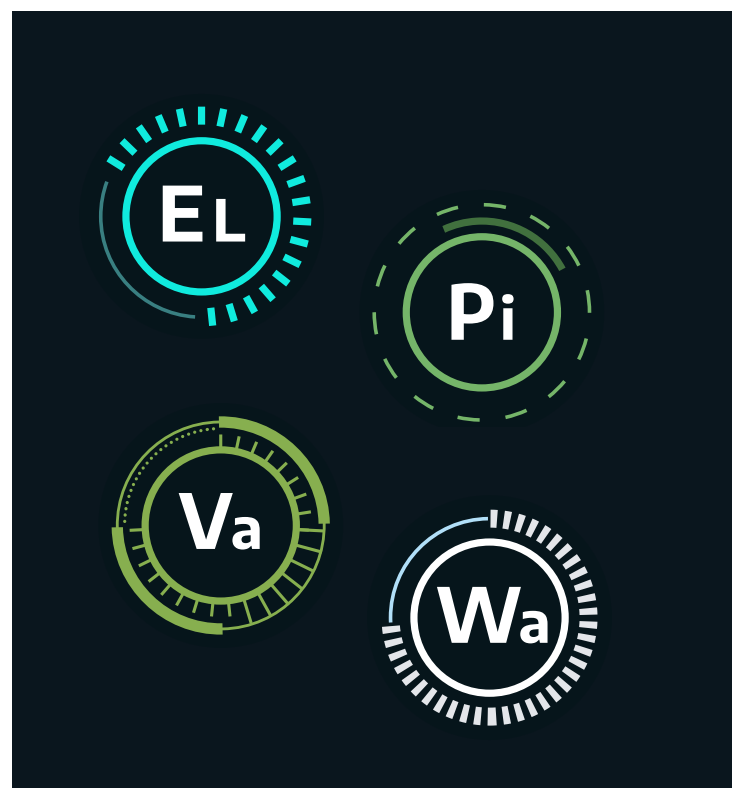
data. How and where the data was collected, judging if an issue is ICS-related or not, and even our definition of public exploit all introduce bias. While the data was collected in good faith, the reader should understand that the data set is likely imperfect as any such data set would be.

PUBLIC ICS/OT EXPLOITS

WHY CARE ABOUT PUBLIC ICS/OT EXPLOITS AT ALL?

The IT world has long been plagued by public exploits being used by malicious adversaries. High profile hacks such as those experienced by Equifax²³, FedEx²⁴, and Maersk²⁵ relied on public exploits. Metasploit, the open source exploitation framework maintained by Rapid7, provides exploits that are adopted by threat actors²⁶. Botnets incorporate dozens of public exploits into their scanning engines²⁷. And private companies like GreyNoise²⁸ and Bad Packets²⁹ have spun up with the sole mission of monitoring vulnerability scanning and exploitation in the wild.

The ICS/OT world is not isolated from these issues. Dragos-tracked activity groups such as VANADINITE³⁰, ELECTRUM³¹, WASSONITE³², and PARISITE³³ use public exploits. Shodan's ICS Radar³⁴ proves ICS assets are being exposed to the internet, and GreyNoise has found³⁵ malicious actors are scanning for ICS equipment. The Dragos 2020 Year In Review³⁶ noted that 100% of our incident response cases involved adversaries accessing the ICS network from the internet.



Given the slow patch cycles within ICS networks, a public exploit is even more valuable to an adversary as the vulnerability is likely to remain unpatched for a longer period. Defenders that track which vulnerabilities have public exploits can prioritize remediation or mitigation efforts and block easy wins for the adversary.

PUBLICATION TRENDS

CVE publication has been on a general upward trend over the last two decades and each of the last four years have set new records for CVEs published³⁷. A very similar trend is observed over the last decade of public ICS/OT exploits. Below is a histogram that sorts the exploits by year of publication.

Public ICS/OT Exploits Publication Year

For Dragos Tracked Vulnerabilities Published From 2010 to Early 2021

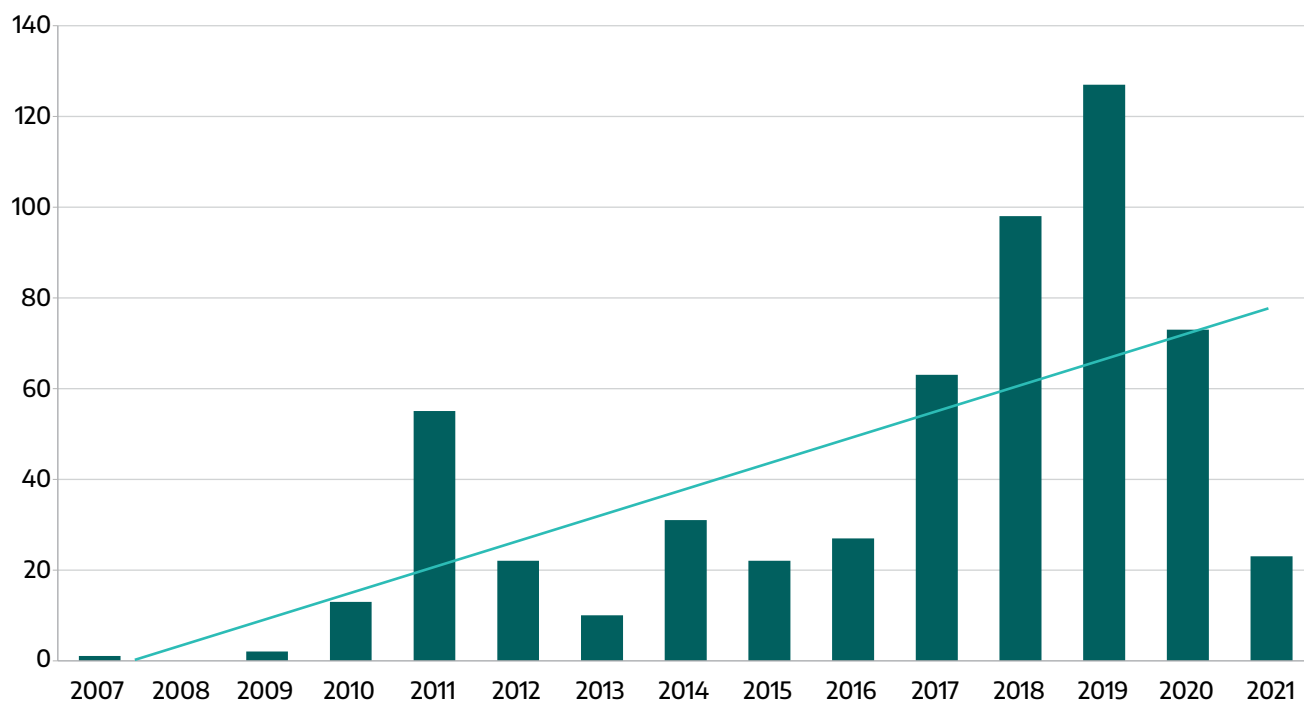


Figure 2: Public ICS/OT exploits tracked by Dragos sorted by year of publication.

Our data shows a clear upward trend in public exploits over the last decade. However, exploits are not necessarily published at the same time as the corresponding CVEs. For example, CVE-2016-5809³⁸ was published in February 2017, but an exploit³⁹ was not published until May 2018. As such, it is useful to consider the publication date of the exploited CVE as well.

Public ICS/OT Exploits and CVE Publication Year

For Dragos Tracked Vulnerabilities Published From 2010 to Early 2021

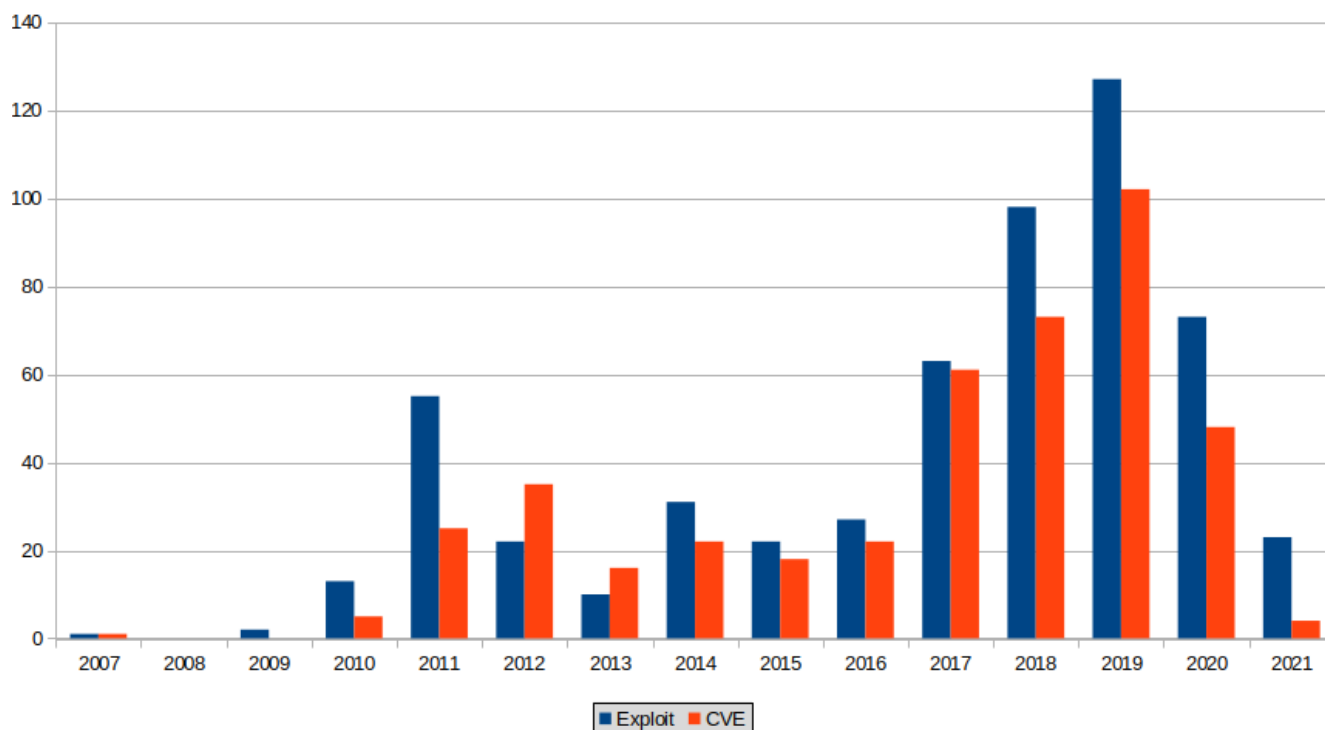


Figure 3: Public ICS/OT exploits and CVEs tracked by Dragos sorted by year of publication.

Figure 3 shows the same upward trend but calls additional attention to 2011. This histogram shows 2011 as the only year the number of public ICS/OT exploits significantly exceeded the exploited CVE count. This is driven by the work of a single individual: Luigi Auriemma⁴⁰. Luigi authored nearly 40 exploits in 2011, all for vulnerabilities he discovered. Many of which would not receive CVE status until following years. Furthermore, 10 of the 2011 exploits were developed by others for vulnerabilities that Luigi found. Which means he was involved in approximately 90% of the ICS/OT exploits published in 2011. Proof that a single individual can make waves in the ICS/OT space.

Figure 2 and **Figure 3** also make it unclear if 2020 was a down year or if 2018 and 2019 were outliers. 2020 does fit the trend line on **Figure 2**, but in **Figure 3** you can see the number of exploits with a published CVE for 2020 is also below 2017 levels. Taking into account the total number of ICS/OT vulnerabilities may clarify what is happening in 2020.

Exploited ICS/OT CVEs and All Dragos Tracked ICS/OT CVE Publications For Dragos Tracked Vulnerabilities Published From 2010 to Early 2021

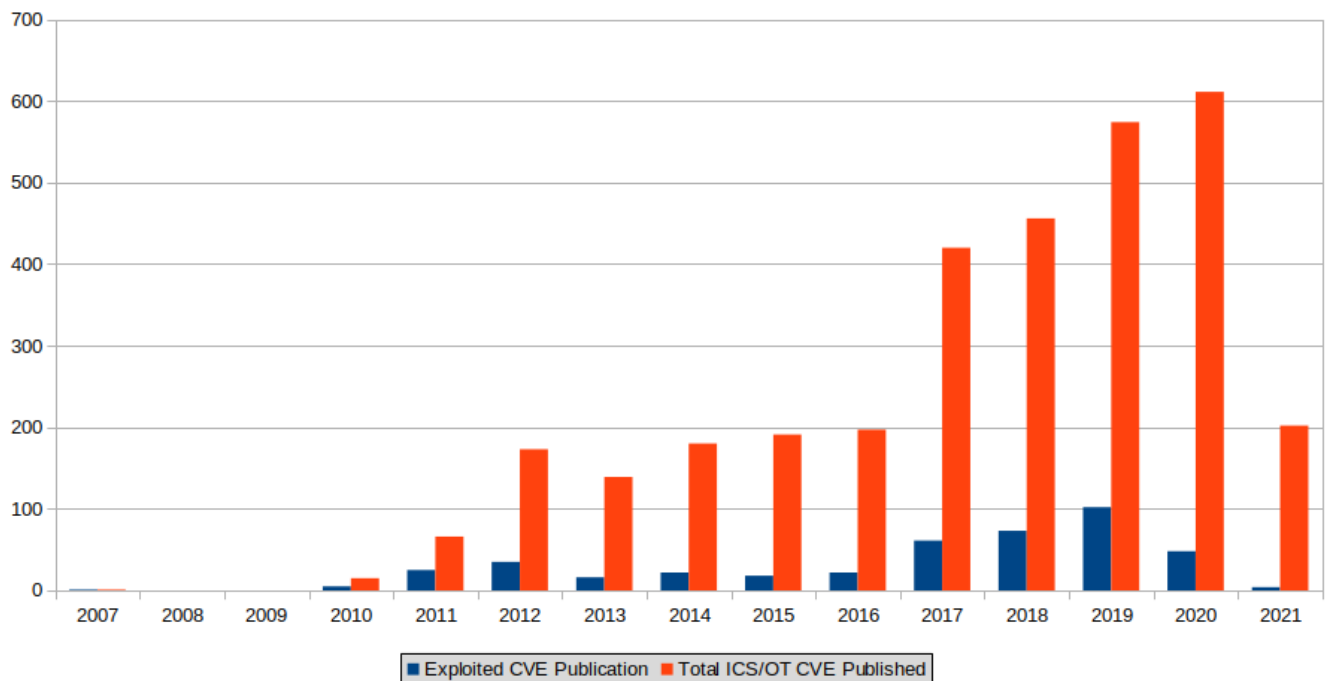


Figure 4: Total ICS/OT vulnerabilities and CVEs with public exploits sorted by year published.

Figure 4 indicates 2020 may very well be a down year. The histogram flags 2020 as the year with the most ICS/OT vulnerabilities, but there is a significant drop in CVEs with public exploits. This is perhaps easier to understand as a percentage.

Year	Percentage of ICS/OT CVEs with a Public Exploit
2010	33%
2011	38%
2012	20%
2013	12%
2014	12%
2015	9%
2016	11%
2017	15%
2018	16%
2019	18%
2020	8%

Table 1: Percentage of ICS/OT CVEs with public exploits.

A single year is not a trend, but 2020 marks a significant drop in published exploits. Casting about for explanations, the possible emergence of a new zero day market seemed plausible. For an independent vulnerability researcher, disclosing vulnerabilities to ICS vendors can be quite tedious. Their vulnerability disclosure programs are often immature and their Product Security Incident Response Teams (PSIRT) are typically understaffed. Coordinated disclosure can take years. Dragos has many aging zero days simply waiting for the vendors to coordinate advisories. It is far easier for a researcher to sell the vulnerability to an exploit broker and move on.

However, Dragos has not found that a new market has opened in 2020. The more public zero day acquisition organizations (Zerodium⁴¹, SSD Secure Disclosure⁴², COSEINC⁴³) do not advertise acquisition of ICS/OT-specific issues. Although we have little new insight into private zero day brokers, historically they have not shown interest⁴⁴, either. Nor have ICS/OT organizations started new bug bounty programs on HackerOne⁴⁵ or Bugcrowd⁴⁶. Zero Day Initiative⁴⁷ (ZDI) is the only well-known zero day acquisition organization that acquires ICS/OT vulnerabilities, but they have been doing that for over a decade.

Instead, Dragos noticed that ZDI has recently acquired a higher percentage of ICS/OT vulnerabilities.

Public exploits for ICS/OT vulnerabilities disclosed through ZDI have historically been quite low. This is likely due to ZDI's "right to republish"⁴⁸ agreement with the researcher being quite restrictive, which does not allow the researcher to publicly publish vulnerabilities ZDI has already purchased.

ZDI takes weeks to evaluate and purchase vulnerabilities. They also follow a 120-day disclosure policy⁴⁹ that can be stretched even longer. As such, all of the vulnerabilities published thus far in 2021 (data is up to early April) were purchased in 2020. An increased utilization of ZDI by vulnerability researchers does plausibly explain the dip in exploits in 2020. If this trend continues, 2021 should remain at 2020 levels even if the overall CVE count increases.

Year	Percentage of ICS/OT CVE Initially Acquired by ZDI
2010	7%
2011	8%
2012	5%
2013	0%
2014	21%
2015	7%
2016	23%
2017	10%
2018	25%
2019	14%
2020	17%
2021 (incomplete year)	48%

Table 2: Percentage of ICS/OT CVE disclosed through ZDI

Year	Percentage ZDI ICS/OT CVE With Public Exploits
2010	0%
2011	0%
2012	33%
2013	3%
2014	43%
2015	0%
2016	4%
2017	24%
2018	4%
2019	0%
2020	6%
2021 (incomplete year)	0%

Table 3: Percentage of ICS/OT ZDI CVEs with public exploits

The impact of the dip is both good and bad for the ICS defender. The bad part is that many vendors rely on Proof of Concept (PoC) exploits to develop and enhance their security products. Without them, security products will not get enhancements that might prove crucial during an incident. The good part is that adversaries will not be able to grab the exploits off the shelf and use them. Although, motivated adversaries are perfectly willing to do the vulnerability analysis required to develop the exploits themselves. Whether it is a net win or net loss is a heavily contested point within information security.

AFFECTED VENDORS

The range of vendors targeted by the nearly 600 exploits is impressive. Dragos found the ICS/OT exploits affect more than 110 vendors. Although, 7 vendors have attracted nearly 40% of the published exploits: Siemens, Schneider Electric, Rockwell Automation, Moxa, Microsoft, Allen-Bradley, and Advantech.

Vendors Affected By Tracked Exploits

For Vulnerabilities Published From 2010 to Early 2021

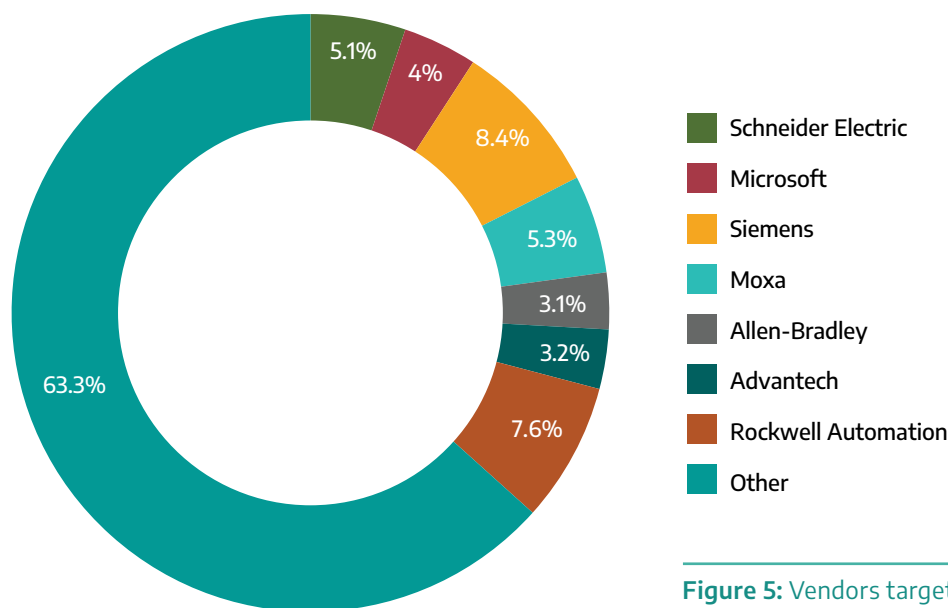


Figure 5: Vendors targeted by public ICS/OT exploits.

The companies highlighted in **Figure 5** have products widely deployed within ICS/OT networks, so it is no surprise that they have attracted the bulk of public exploits. The **Other** category includes a range of vendors from traditional ICS vendors like General Electric to less traditional like Palo Alto.

Vulnerabilities exist in every product and public exploits should be expected. Most of the vendors at the top of the affected vendors list openly publish detailed security advisories, mitigation guidelines, and impact statements. Their publications provide insights that help the security

community and their customers understand the risk the vulnerabilities pose. It just so happens that this openness makes exploit development easier.

As a defender, the take-away should be to better engage in these vendor communications. For example, if your organization deploys Moxa devices then it's worthwhile to monitor Moxa's publicly available security advisory page.

VIEWED THROUGH THE PURDUE MODEL

When discussing ICS/OT exploits, it is important to understand the potential impact the exploit might have on the industrial process. For this, we rely on the Purdue Model. In **Figure 6**, the public ICS/OT exploits have been mapped to the Purdue Level of the affected software/device.

Exploits Per Purdue Level

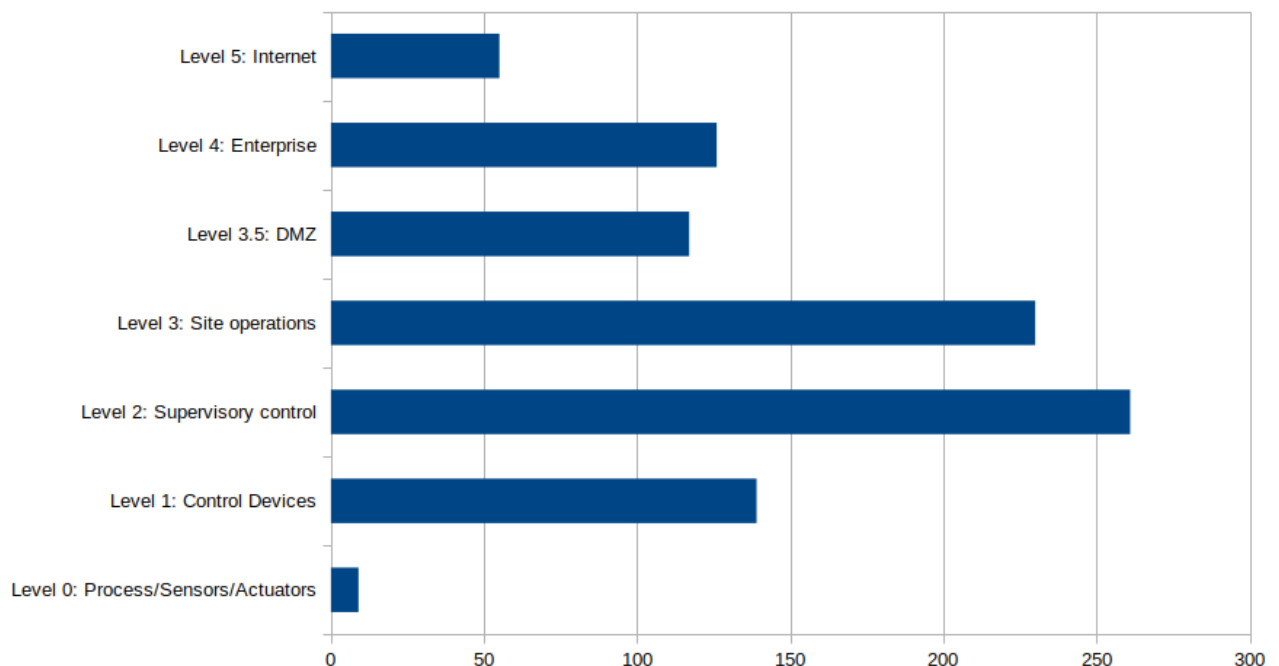


Figure 6: Public ICS/OT exploits mapped to impacted Purdue Level.

As this paper discusses ICS/OT exploits, it is unsurprising to see the majority of exploits map within the ICS network (Levels 1, 2, and 3). An observant reader might notice more exploits are accounted for in **Figure 6** than **Figure 2**. That is because affected software can be found at more than one Purdue Level.

For example, an exploit that targets [OpenSSL](#) affects systems on levels 1-5.

Public exploits for Purdue Level 3 systems are of particular interest because they sometimes serve as the initial access point into the ICS network. The Level 3 device could be as simple as an RDP jump box or something

more complicated like a VPN appliance. Either way, exploitation of that type of system earns an adversary broader network access into the ICS network. Furthermore, control of the entry point could allow the adversary to indirectly affect a loss of view⁵⁰ and loss of control⁵¹ on the ICS process.

Of course, with broader network access, Level 2 exploits also become quite interesting

as Level 2 systems act in a supervisory capacity to the industrial process. Exploitation of Level 2 systems could result in extreme failures beyond loss of view and loss of control, such as manipulation of view⁵² and manipulation of control⁵³. Meaning, the attacker could potentially directly affect the industrial process from a Level 2 vantage point.



IMPACTFUL EXPLOITS

Understanding the actual impact of ICS/OT exploits and how that might eventually affect the industrial process is crucial. While a denial of service (DoS) attack in the enterprise might be an annoyance, a denial of service of a Purdue Level 1 or 2 system in the ICS network might be dangerous. For example, exploitation of CVE-2015-5734, a DoS issue ELECTRUM attempted to use via CRASHOVERRIDE⁵⁴, would have allowed the adversary to disable the digital relay. Without the relay, the industrial process may be influenced into (or run away into) a dangerous state resulting in physical damage to key transmission equipment.

Because different bug classes can have substantially different impacts depending on the affected Purdue Level, it is useful to break out each of the types of exploits Dragos tracks at each Purdue level.

Tracked Exploit Impact By Category and Purdue Level

For Vulnerabilities Published From 2010 to Early 2021

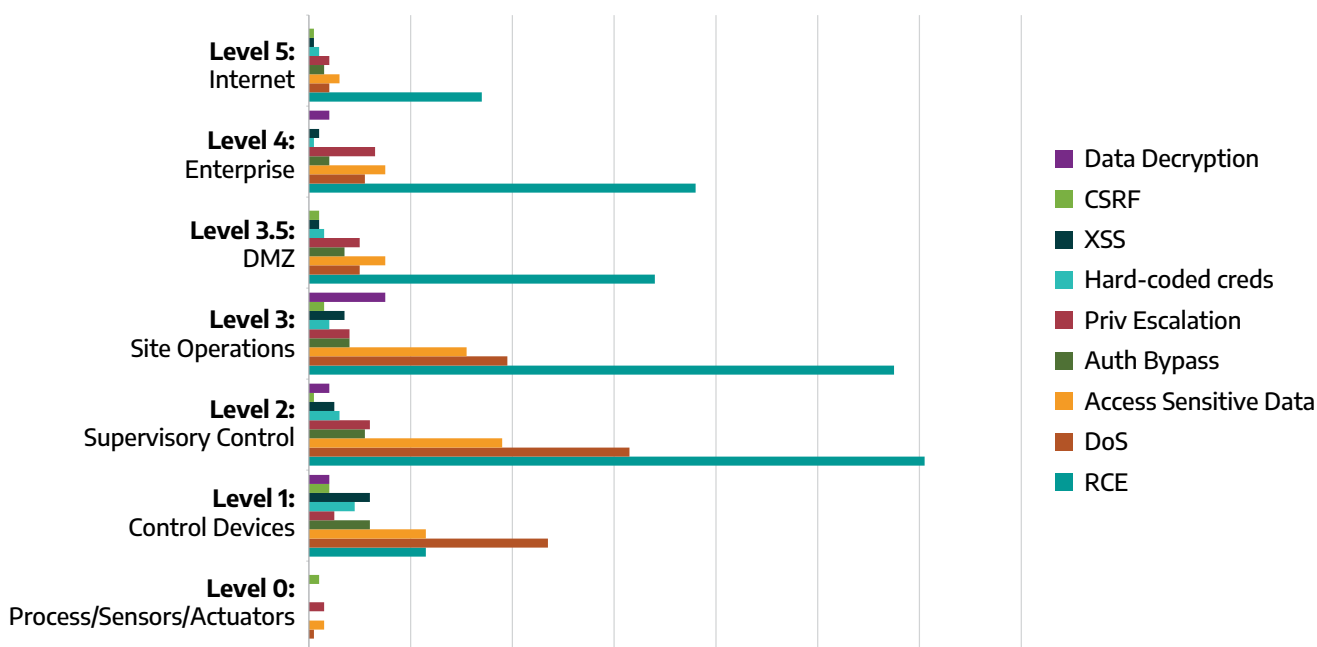


Figure 7: Impacted Purdue Level broken down into bug classes.

Remote code execution⁵⁵ (RCE) is the most likely impact for all exploits for level 2 and above. An exploit developer is more likely to spend their time developing and publishing an RCE exploit over any other class due to the significant impact it achieves at any Purdue Level. However, Level 1 devices are harder for a researcher to obtain and introducing tools to the device to aid in exploit development is difficult, and due to the lack of security features (insecure by design⁵⁶), developing a DoS "exploit" on a Level 1 device can be as simple as invoking normal functionality (for example, to reboot the controller). Also, as discussed, DoS can be very impactful in the ICS/OT

environment. As such, DoS exploits are the most common Level 1 impact.

Generically describing the impact of RCE exploits on the industrial process is difficult as every system has a unique role within the process. But it is reasonable to say that RCE exploits provide the ability to pivot and persist within an ICS network and are all but required to execute both Stage 1 and Stage 2 of the ICS Cyber Kill Chain⁵⁷. **Figure 8** addresses how RCE is achieved against ICS/OT-related systems.

RCE Exploit Method

For Vulnerabilities Published From 2010 to Early 2021

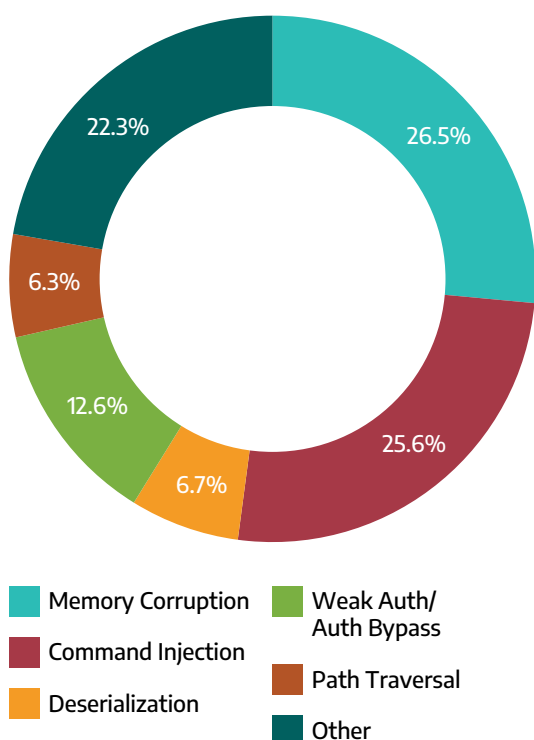


Figure 8: Bug class used for remote code execution.

Memory corruption leads the way on the complete dataset. However, writing RCE exploits for memory corruption issues has become significantly harder over the years. If the data set is limited to exploits written for vulnerabilities published in 2017 and later, the chart looks like this:

RCE Exploit Method

For Vulnerabilities Published From 2017 to Early 2021

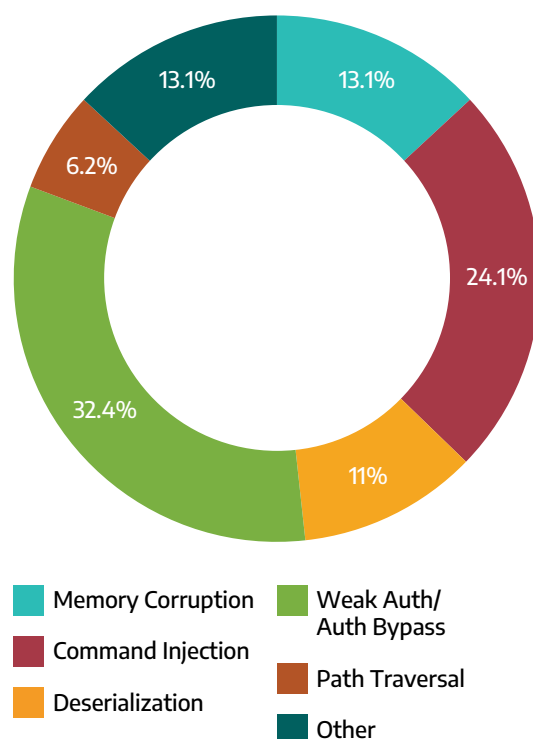


Figure 9: Bug classes used for remote code execution for public ICS/OT exploits published from 2017 onwards.

More recent RCE exploits are less likely to exploit a memory corruption vulnerability. Of course, this does not necessarily mean that modern mitigations are preventing RCE on memory corruption issues. The drop could just be indicative of the additional time and know-how that the mitigation bypass requires, something that might not be worthwhile to a

researcher. This is somewhat supported by the rise in command injection exploits, as they often require minimal effort to write and represent minimal time commitment.

Regardless of bug class, the breakdown by Purdue level shows that there are highly impactful public ICS/OT vulnerabilities at every level. Prioritizing patching and remediation

at Level 3, where the initial entry into the ICS network happens, is a great start. But if Level 3 is breached, it is important to know that the lower levels are also significantly impacted by public ICS/OT exploits. Time and resources permitting, it is ideal for defenders to prioritize remediation and mitigation at these lower levels as well.

MOSTLY USELESS

Of course, some of the public ICS/OT exploits are useless. For example, a cross site request forgery⁵⁸ (CSRF) against a PLC is unlikely to ever be used in the wild, because it requires the victim to be logged into the PLC’s web interface and to navigate to a malicious site (or click on a malicious link). It also requires the attacker to be able to craft URLs that address the victim’s PLC. That is an unlikely scenario. Similar criticisms can be leveled at cross site scripting⁵⁹ (XSS) exploits. **Table 4** shows that CSRF and XSS exploits occur at every Purdue level:

Level	Percentage of Public Exploits That Are CSRF or XSS Exploits Initially Acquired by ZDI
5	4%
4	2%
3.5	3%
3	4%
2	2%
1	9%
0	22%

Table 4: Percentage of public exploits that leverage XSS or CSRF by Purdue

The Common Vulnerability Scoring System⁶⁰ (CVSS) version 2.0 has an “access complexity” (AC) component⁶¹ which captures the special

circumstances that must exist to exploit a vulnerability. The component has three ratings:

- **Low:**
The vulnerability can be exploited at will.
- **Medium:**
Exploitation requires some special circumstances such as user interaction (e.g. a clicked link), additional information, or a non-default configuration.
- **High:**
Exploitation requires special circumstances such as man in the middle, extensive social engineering, or rarely used configurations.

Both XSS and CSRF are assigned an AC of medium because they require user interaction and additional information for successful exploitation.

Another good example of an exploit that has high access complexity is CVE-2020-0601⁶², also known as “CurveBall” or “Chain of Fools”⁶³. CurveBall is the result of Windows improperly validating the signature of certificates using elliptic curve cryptography (ECC). One of the best exploits for CurveBall is Saleem Rashid’s BADECPARAMS⁶⁴, in which an HTTP server claims to be nsa.gov, verified by a PayPal certificate, while presenting the user with a Rick Roll video on YouTube.

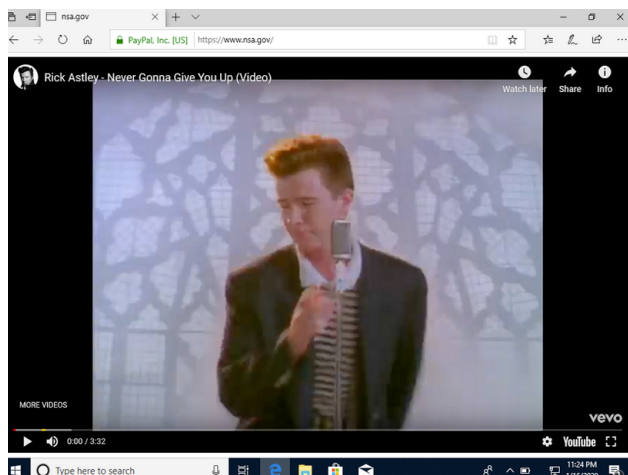


Figure 10: BADECPARAMS proof of concept screenshot. Sourced from github.com/saleemrashid/badecparams

There is no doubt that BADECPARAMS is a great hack. But it lacks value within the context of attacking an ICS/OT network. The exploit requires the adversary to have a man-in-the-middle position or to trick a user into clicking a link. Those are unreasonable conditions within an ICS network.

In fact, within our dataset, every Purdue level has a significant number of public exploits that have an access complexity of medium or higher.

AUTHOR AFFILIATION

The public ICS/OT exploits tracked by Dragos are developed for all Purdue levels and affect a wide range of technologies. The result is that the exploits encompass a lot of unique security knowledge. Where is that knowledge coming from? Who are the people behind the exploits? Unfortunately, when broken down by exploit author, the only insight gained is **a lot of people have helped create these exploits!** Almost 250 unique individuals.

Breaking down exploits by the author's sponsoring organization (employer or university) proved a little more interesting. Just under half of the exploits tracked by Dragos were developed in association with a sponsor.

Level	Percentage of Public Exploits With AC of Medium or Higher
5	45%
4	26%
3.5	26%
3	30%
2	28%
1	29%
0	22%

Table 5: Percentage of public exploits with AC of medium or higher

Not all exploits are created equal. Especially within the context of an ICS/OT network. Remediation of public exploits with medium or higher access complexity, the type of exploits that require user interaction, man-in-the-middle position, or unique configurations, should not be a priority. They are likely useless within the confines of an ICS/OT network.

Exploit Author Affiliation

For Vulnerabilities Published
From 2010 to Early 2021

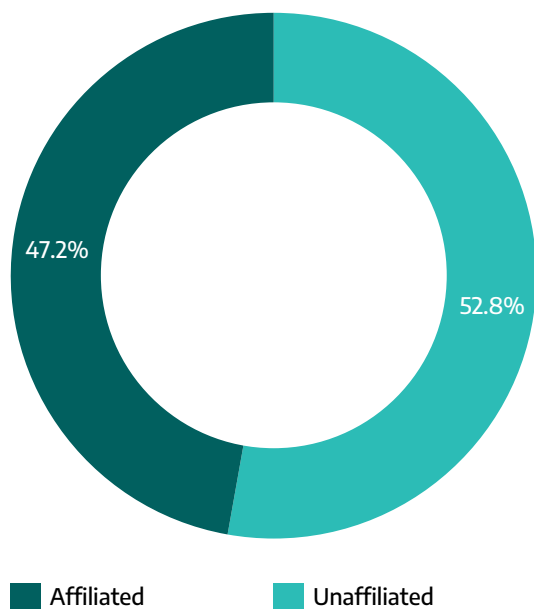


Figure 11: Exploit author affiliation with a sponsor (company or university).

This was a surprising result, as publicly releasing privately developed code is often fraught with bureaucracy and oversight. Of the exploits where the author is affiliated with a sponsor, three companies had employees that authored 50% of the published exploits: Rapid7, Talos, and Tenable.

Exploit Author Sponsors

For Vulnerabilities Published
From 2010 to Early 2021

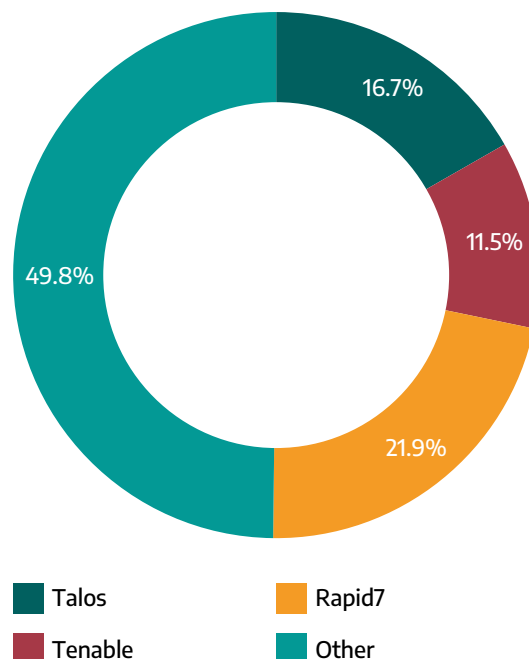


Figure 12: Exploit author sponsors.

The **Other** category is comprised of more than 60 companies and universities, often being credited with 1 to 3 exploits.

Otherwise, looking where Dragos has found exploits, this breakdown makes sense. Rapid7 employees develop exploits for Metasploit, so naturally they should be at the top of the list. Both Talos and Tenable are CVE Numbering Authorities⁶⁵ (CNA) that often issue and publish CVE for original vulnerability research. Both often share PoC exploits. It is useful to note that they are CNA, because MITRE includes “Assigning CNA” in the CVE entry. CVEs assigned by Talos and Tenable are much more likely to have associated public exploits.

CVE-ID	
CVE-2020-13536	Learn more at National Vulnerability Database • CVSS Severity Rating • Fix Information • Vulnerability Details
Description	
An exploitable local privilege elevation vulnerability exists in the file system permissions of the MXViewService, which starts as a NT SYSTEM authority user executes a series of Nod	
References	
Note: References are provided for the convenience of the reader to help distinguish between vul	
<ul style="list-style-type: none"> MISC:https://talosintelligence.com/vulnerability_reports/TALOS-2020-1148 URL:https://talosintelligence.com/vulnerability_reports/TALOS-2020-1148 	
Assigning CNA	
Talos	
Date Record Created	
20200526	Disclaimer: The record creation date may reflect disclosed, or updated in CVE.

Figure 13: CVE Entry for CVE-2020-13536 showing Talos as the assigning CNA

As it turns out, third-party advisories such as those published by Talos and Tenable are the most significant source of public exploits.

Exploit Source For Vulnerabilities Published From 2010 to Early 2021

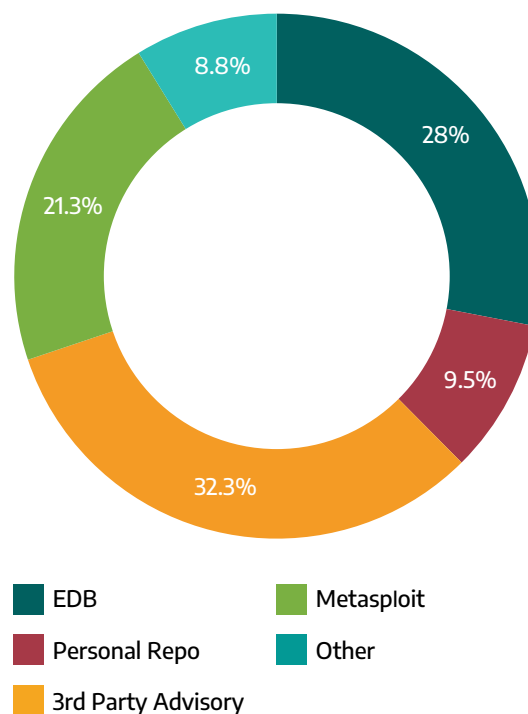


Figure 14: Public ICS/OT exploits source.

Dragos tracks third-party advisories from big companies all the way down to more obscure personal blogs⁶⁷. Scrutinizing the more obscure sources often helps find researcher GitHub or Bitbucket repositories where they have stored even more PoC exploits. Of course, both Metasploit and the Exploit-DB have been exploit clearinghouses for quite some time now. The **Other** category in **Figure 14** breaks down to whitepapers, Twitter, presentations, bug trackers, Full Disclosure⁶⁸, other exploit frameworks, and when all else fails, Packet Storm⁶⁹.

TIME TO FIRST PUBLIC EXPLOIT

Defenders often prioritize remediation of vulnerabilities that have public exploits. It would be useful to be able to predict the time range a defender could reasonably expect a public exploit to appear. Rephrasing into a question, “How long can I wait before a public exploit can be expected for a new publicly disclosed vulnerability?” The date at which a CVE is publicly disclosed, for our purposes, is the NVD published date timestamp.

The complete 2010 to early 2021 data set shows the median public disclosure to public exploit time gap is -1 days. Meaning, typically speaking, if a public exploit is published, it will have been published one day before NVD populated their CVE entry. Given the delay in NVD’s publishing, the reader can understand this to mean that exploits are published around the same time as the initial vendor or researcher advisory.

This may be a poor measure of time to first public exploit for **useful** exploits though. Many of the exploits in our data are developed by the same individual that discovered the vulnerability. Often, vulnerability researchers release PoC exploits to help other researchers understand their work, whether the exploit is useful in a real world setting or not. For lack of a better term, this paper refers to those exploits as vanity exploits. When we remove all vanity exploits from the data set, the median time to first public exploit jumps to 24 days.

Time to First Exploit (Days)

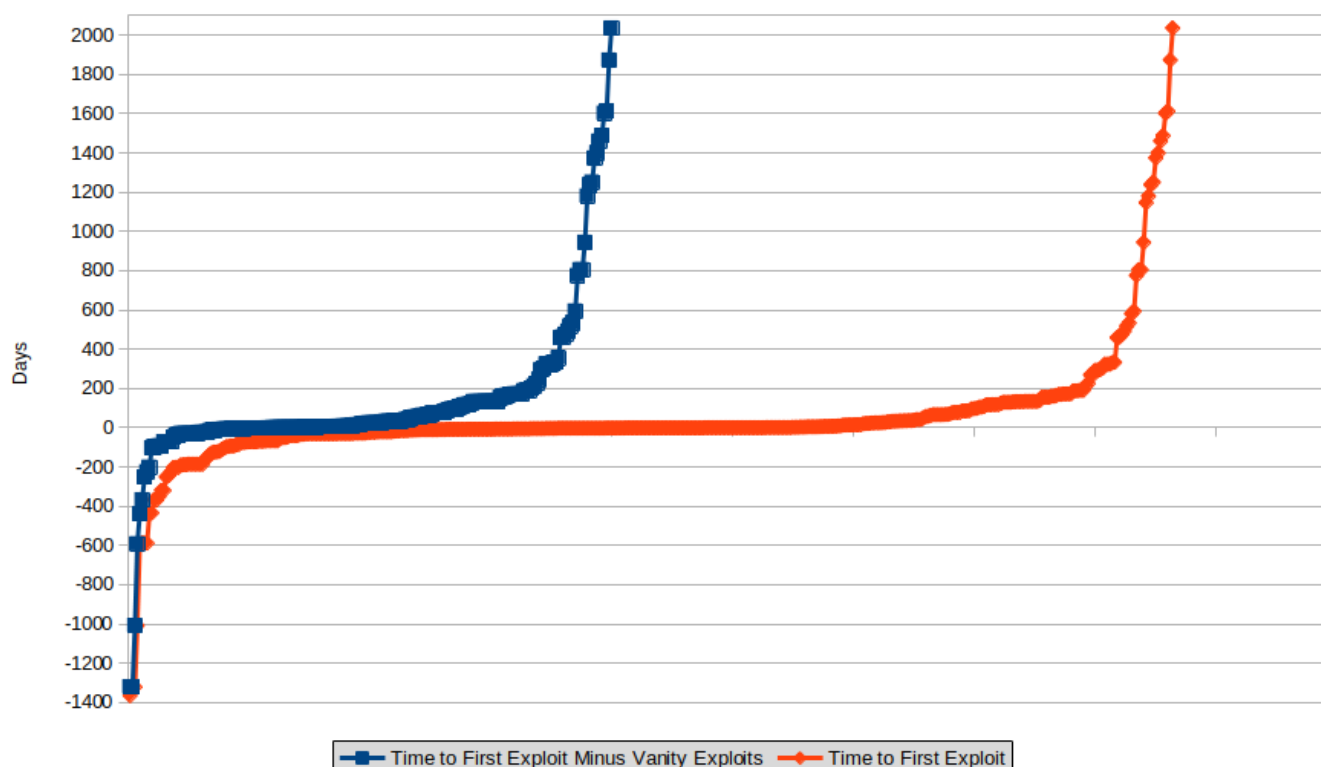


Figure 15: Public ICS/OT exploits release dates plotted around public disclosure.

This may give credence to Google Project Zero's recent adoption of delaying full disclosure for 30 days⁷⁰ after initial vendor disclosure. Although it provides no insight into the time to first private exploit. Regardless, ICS/OT network defenders can reasonably expect that, on average, if a CVE is going to get a public exploit, then it will be released within the first 30 days after initial disclosure.

Of course, there are outliers in the data. For example, this [gist](#) for CVE-2015-7937⁷¹ was published more than 1600 days (about 4.5 years) after Schneider Electric published their initial advisory⁷². In the other direction, CVE-2015-6461⁷³ and CVE-2015-6462⁷⁴ were presented at DEF CON⁷⁵ by Aditya K. Sood in 2015, but were not published to NVD until 2019, nearly a four-year gap between exploitation details being public and NVD publication.

The very early PoC exploits are often immature. They typically need some amount of effort to be included in mature exploitation frameworks like Metasploit⁷⁶. An exploit included in Metasploit is a little more dangerous than a standalone one, as it will benefit from the framework's expansive post-exploitation feature set. As such, Dragos was interested in this time gap as well: public disclosure to when the exploit was merged into Metasploit. If an exploit was eventually ported into Metasploit, the data showed the median time gap from public disclosure to be 31 days.

Patch cycles within ICS networks can greatly exceed these 30 day time gaps. The focus should not be on trying to mitigate or patch all vulnerabilities within that window. That is unreasonable and likely impossible. Instead, if a vulnerability is, for example, 120 days old and still has no public PoC, perhaps it will not get one at all. If that is the case, and the affected component is not internet facing, then the defender might instead focus their remediation and mitigation efforts elsewhere.



IN THE WILD

As stated earlier, public exploits lower the barrier to entry for attackers. But that does not mean public ICS/OT exploits are actually being used. Of the current data set, Dragos tracks only 54, or just under 10%, of the CVEs with public ICS/OT exploits as having been known to be exploited in the wild (including by Dragos-tracked activity groups: PARISITE, VANADINITE, WASSONITE, and ELECTRUM).

ICS/OT-Related CVE Actively Exploited by Purdue Level

For Vulnerabilities Published From 2010 to Early 2021

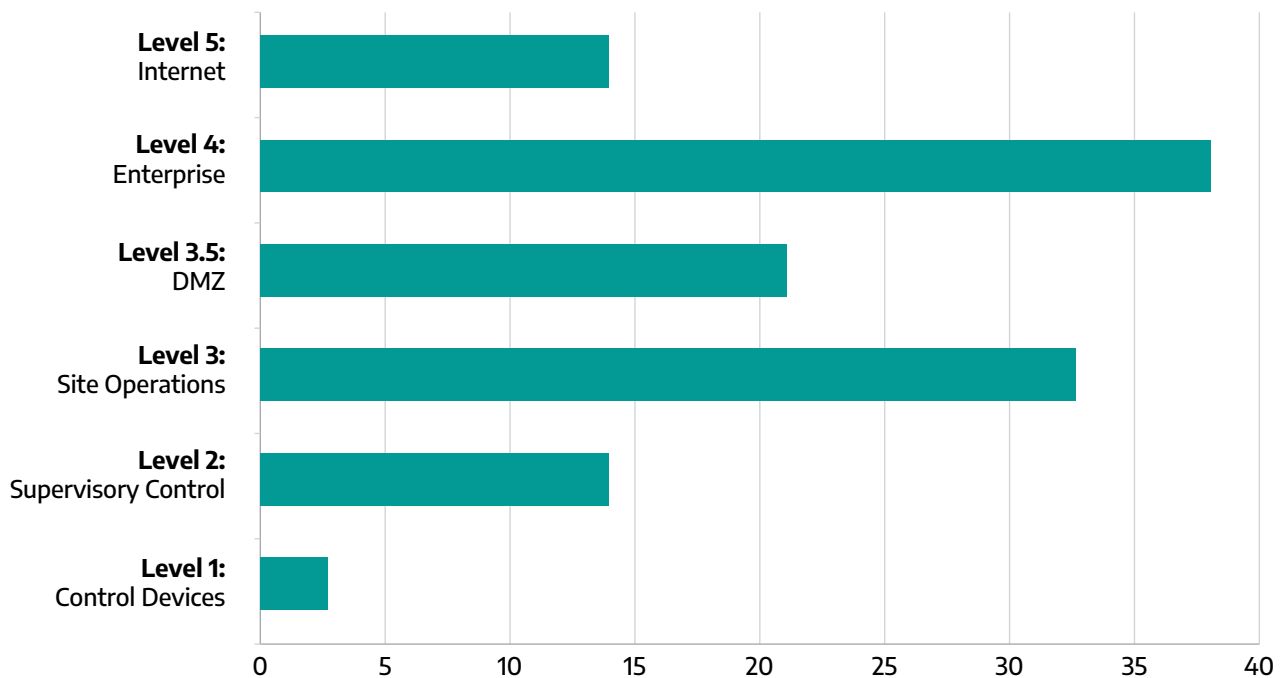


Figure 16: ICS/OT-related CVE with public exploits mapped to affected Purdue Levels.

A 10% “**exploited in the wild**” rate should probably be considered a floor. **Figure 16** tells the story why: visibility in the lower levels of the ICS network (Level 1 and Level 2) is poor. Until we are better able to monitor these levels at scale, we must assume that we are missing a non-negligible amount of exploitation.

Another interpretation of the histogram could be that mitigation and patch prioritization of Level 3 is of utmost importance because that is where exploitation is seen most in an ICS/OT network. An adversary might not need Level 1 or Level 2 exploits since taking control of a site operations or supervisory system will often give the adversary control of the Level 1 devices by using the programming software and other interfaces present on the system. The Oldsmar incident⁷⁷ is a great example of an adversary affecting the industrial process via unauthorized access of a supervisory HMI. Although, that is also an intuitive result of the Purdue Model, so it may not be an interesting takeaway.

CONCLUSION

The ICS/OT public exploit world has been active over the last decade and continues to be so. Many individuals and organizations are actively developing these ICS/OT-impacting exploits, and a small percentage of them are used in the wild. However, there are so many ICS/OT exploits published that every couple of months or so, it is reasonable to expect that one of them will be adopted by a threat actor and used in the wild. As such, it's imperative to track public exploits to help determine which vulnerabilities should be remediated or mitigated. The following advice may prove useful to that end:

- **Public exploits are generally published within the first 30 days after disclosure.** Vulnerabilities that have not been remediated but are outside of the 30-day window may be lower priority.
- **Evaluate the source of the CVE under consideration.** Some organizations are known to publish PoC exploits with the CVE. CVEs discovered by security researchers are far more likely to have associated public exploits.
- **Understand the impact of the exploit.** Exploits that only affect the ICS/OT network but require user interaction or man-in-the-middle can be deprioritized.
- **Do not completely ignore impactful Level 1 and Level 2 public exploits.** There is insufficient visibility that deep into the ICS/OT network to know if those exploits are being used in the wild or not.

REFERENCES

- 1 ICS Cybersecurity Year in Review 2020 – [Dragos](#)
- 2 What is the Purdue Model for ICS Security – [ZScaler](#)
- 3 Ecava IntegraXor SQL Injection Remote Code Execution – [Tenable](#)
- 4 Integraxor Advisory – [Luigi Auriemma](#)
- 5 Talos Vulnerability Report – [Cisco Talos](#)
- 6 Rockwell Automation Allen-Bradley PowerMonitor 1000 – Incorrect Access Control Authentication Bypass – [Exploit Database](#)
- 7 GNU Wget – [gnu.org](#)
- 8 Netcat – [nc110.sourceforge.io](#)
- 9 OpenSSL – [openssl.org](#)
- 10 Exploit Database – [exploit-db.com](#)
- 11 CANVAS – [Immunity, Inc.](#)
- 12 PARISITE – [Dragos](#)
- 13 Initial Access – [MITRE ATT&CK for ICS](#)
- 14 Recommendations Following the Oldsmar Water Treatment Facility Cyber Attack - [Dragos](#)
- 15 EternalBlue – [Wikipedia](#)
- 16 Microsoft Security Bulletin MS17-010 – Critical – [Microsoft](#)
- 17 Exploitation of Remote Services – [MITRE ATT&CK for ICS](#)
- 18 National Vulnerability Database – [NIST](#)
- 19 ICS-CERT Advisories – [Cybersecurity & Infrastructure Security Agency](#)
- 20 Honeywell Experion PKS Directory Traversal Vulnerability – [ICS-CERT](#)
- 21 CVE-2007-6483 – [National Vulnerability Database](#)
- 22 SafeNet Sentinel Protection Server 7.x/Keys Server 1.0.3 - Directory Traversal – [Exploit Database](#)
- 23 LiquidWorm – [Exploit Database](#)
- 24 The Equifax Data Breach – [U.S. House of Representatives Committee on Oversight and Government Reform](#)
- 25 2019 Annual Report – [FedEx Corporation](#)
- 26 The cost of malware infection? \$300 million for Maersk – [Digital Guardian](#)
- 27 Microsoft works with researchers to detect and protect against new RDP exploits – [Microsoft](#)
- 28 Mirai Variant ECHOBOT Resurfaces with 13 Previously Unexploited Vulnerabilities – [Unit42](#)
- 29 GreyNoise – [greynoise.io](#)
- 30 Bad Packets – [badpackets.net](#)
- 31 VANADINITE – [Dragos](#)
- 32 ELECTRUM – [Dragos](#)
- 33 WASSONITE – [Dragos](#)
- 34 Shodan ICS Radar – [Shodan](#)
- 35 Phoenix Contact PLC Scanner – [GreyNoise](#)
- 36 ICS Cybersecurity Year In Review 2020 – [Dragos](#)
- 37 Statistics Results – [National Vulnerability Database](#)
- 38 CVE-2016-5809 – [National Vulnerability Database](#)

REFERENCES

- 39 PowerLogic/Schneider Electric IONXXXX Series – Cross-Site Request Forgery – [Exploit Database](#)
- 40 Luigi Auriemma – [alugi.altervista.org](#)
- 41 Our acquisition program – [Zerodium](#)
- 42 SSD Secure Disclosure – [ssd-disclosure.com](#)
- 43 Pwnorama – [COSEINC](#)
- 44 Hacking Team: a zero-day market case study – [tsyrkleyvich.net](#)
- 45 HackerOne Bug Bounty – [HackerOne](#)
- 46 Managed Bug Bounty – [Bugcrowd](#)
- 47 Zero Day Initiative – [zerodayinitiative.com](#)
- 48 Zero Day Initiative Researcher Agreement – [Zero Day Initiative](#)
- 49 Disclosure Policy – [Zero Day Initiative](#)
- 50 Loss of View – [MITRE ATT&CK for ICS](#)
- 51 Loss of Control – [MITRE ATT&CK for ICS](#)
- 52 Manipulation of View – [MITRE ATT&CK for ICS](#)
- 53 Manipulation of Control – [MITRE ATT&CK for ICS](#)
- 54 Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – [Dragos](#)
- 55 The ability for an adversary to introduce and execute arbitrary code or commands over the network.
- 56 Insecure by design: What you need to know about defending critical infrastructure – [CSO](#)
- 57 Industrial Control System Cyber Kill Chain – [SANS](#)
- 58 Cross Site Request Forgery – [OWASP](#)
- 59 Cross Site Scripting – [OWASP](#)
- 60 Common Vulnerability Scoring System – [first.org](#)
- 61 CVSS v2 Complete Documentation Section 2.1.2 Access Complexity (AC) – [First.org](#)
- 62 CVE-2020-0601 – [MITRE](#)
- 63 A Technical Analysis of CurveBall – [TrendMicro](#)
- 64 BADECPARAMS – [github.com](#)
- 65 CVE Numbering Authorities – [MITRE](#)
- 66 CVE-2020-13536 – [MITRE](#)
- 67 CVE-2016-4513 Schneider Electric PowerLogic PM8ECC XSS – [Mogozobo](#)
- 68 Full Disclosure Mailing List – [seclists.org](#)
- 69 Packet Storm – [packetstormsecurity.com](#)
- 70 Policy and Disclosure: 2021 Edition – [Project Zero](#)
- 71 CVE-2015-7937 – [National Vulnerability Database](#)
- 72 Schneider Electric Security Notification – [Schneider Electric](#)
- 73 CVE-2015-6461 – [National Vulnerability Database](#)
- 74 CVE-2015-6462 – [National Vulnerability Database](#)
- 75 Dissecting the Design of SCADA Web HMIs: Hunting Vulns – [DEFCON 23](#)
- 76 Metasploit – [github.com](#)
- 77 Recommendations Following the Oldsmar Water Treatment Facility Cyber Attack – [Dragos](#)

ABOUT DRAGOS

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

**TO LEARN MORE
ABOUT DRAGOS AND
OUR TECHNOLOGY,
SERVICES, AND THREAT
INTELLIGENCE FOR
THE INDUSTRIAL
COMMUNITY,
PLEASE VISIT**

www.dragos.com.



THANK YOU