



# YEAR IN REVIEW — 2018

INDUSTRIAL CONTROLS  
SYSTEM VULNERABILITIES



The Dragos Intelligence team analyzes ICS-specific vulnerabilities from 2018 and provides impacts, risks, and mitigation strategies.

## CONTENTS

---

- 1 EXECUTIVE SUMMARY
  - 2 KEY FINDINGS
  - 3 RECOMMENDATIONS
  - 4 OPERATIONS IMPACT
  - 5 PERIMETER IMPACT
  - 6 VULNERABILITY DISCLOSURES OVER TIME
  - 7 MITIGATION ADVICE VERSUS EXPLOITABILITY
  - 8 CONCLUSION
-



## EXECUTIVE SUMMARY

In 2018, Dragos tracked 204 public vulnerability advisories with an impact on industrial control systems (ICS). The majority of these vulnerabilities affected parts of the control system that are not exposed to corporate networks.

The advisories covered 443 individual Common Vulnerability and Exploit identifiers (CVEs), and Dragos found that one third of these had errors in describing and rating the severity of reported vulnerabilities. Additionally, many vulnerability advisories provided limited or insufficient mitigation information. However, the number of vendors self-reporting vulnerabilities continues to increase, with fewer errors than the overall advisories, and researchers are more frequently collaborating with vendors to disclose security issues.



## KEY FINDINGS

**82%** of advisories covered products which reside deep within a control system network, or which have no direct control systems interaction at all.

**68%** of advisories covered network-exploitable vulnerabilities. However only 28% of these network-exploitable advisories provided mitigation advice sufficient to take effective action.

**32%** of all CVEs in the ICS space had errors in the Common Vulnerability Scoring System (CVSS) vector and numeric score. This means that the public advisory incorrectly described the vulnerability and its severity.

**18%** of vendor-produced advisories had errors in the CVSS score, versus 32% overall.

On average, Dragos reviewed **17** relevant security advisories per month.



# RECOMMENDATIONS



BETTER ICS  
VULNERABILITY  
ADVISORIES



BETTER UPDATE  
PROCESSES



PROMOTE SELF-  
REPORTING AND  
WORKING WITH  
VENDORS

---



## Better ICS Vulnerability Advisories

ICS vulnerability assessments as published are frightfully inadequate and fail to provide asset owners and operators with meaningful guidance.

Advisories continue to provide generic advice for network-exposed and local-access security vulnerabilities: “Deploy firewalls and use only trusted networks.” However, if end users cannot apply patches due to scheduled patch cycles, inability to accept downtime, or various other reasons, this generic advice is not meaningful.

**Recommendation: Advisories must provide reasonable alternative options. The advice mentioned above does not make sense for local vulnerabilities and is not actionable for network-exposed vulnerabilities. Advisories should contain information pertaining to the service exposing the vulnerability and provide a list of networked systems that require access to the service for proper functionality, either in the advisory or via references to technical documentation.**

Public advisories continue to ignore industrial impacts, and never provide a meaningful likelihood of exposure. These two key pieces of information help an end user determine whether an advisory requires immediate action or if it can be addressed at a later time.

**Recommendation: Add “Likelihood of ICS Border” ratings to advisories based on a reference architecture such as the Purdue Model.<sup>1</sup>**

---

1. The Purdue Enterprise Reference Architecture:

<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.194.6112&rep=rep1&type=pdf>

15% of advisories cover local file vulnerabilities, either project file format vulnerabilities or DLL hijacking. On a well-architected control system network, these are considered low risk.

**Recommendation: Provide more tailored advice for local file vulnerabilities. This includes using operating system features to restrict inbound and outbound network communications on affected systems, or providing file type or file extension information that may be used for scanning services.**

34% of the network-exploitable advisories covered industrial-specific protocols. The remainder were generic protocols such as HTTP, FTP, and proprietary but not ICS-specific protocols. This is likely because security testing tools exist for generic IT protocols. There is still a lack of tools for assisting testers in ICS-specific testing.

**Recommendation: Increase focus on control systems protocol issues and development of ICS protocol testing tools.**

Several high-profile advisories repeated previously-disclosed issues. These included advisories against field devices. Typically, these are vulnerabilities in related products from the same vendor, but sometimes the overlap is the same exact product.

**Recommendation: Survey for vulnerabilities in related products before publishing new advisories and reserving new CVEs. Affected vendors should internally research and self-report when an existing vulnerability affects additional products.**

32% of public advisories contain basic factual errors, including incorrect CVSS scores. This error rate is not evenly distributed. Dragos reviewed external bug reporting organizations and identified significantly worse advisories: 56% of advisories reported through one third-party organization contained incorrect CVSS scores.

**Recommendation: Review FIRST's CVSS specification document<sup>2</sup>, and verify CVSS scores of published advisories before publication.**

Just 10% of all advisories cover an extremely critical intersection: perimeter systems that may be used by an attacker to pivot into the control systems network where exploitation can be achieved with little to no difficulty.

**Recommendation: Increase research on network perimeter systems. This includes firewalls and VPNs used by industrial operators and cross-domain systems such as data historians, OPC servers, and other industrial-focused remote access systems.**

Nearly 72% of advisories cover HMI, Engineering Workstation (EWS), and Field Device/Industrial Networking components. Mitigating vulnerabilities in these types of systems does little to reduce an industrial impact – an attacker that is in a position to target these systems will likely achieve their goal without use of vulnerabilities.

**Recommendation: Focus research on services that are most likely to present attack surface to the corporate network such as those listed above.**

Fewer than half of the EWS and HMI vulnerabilities were network-exploitable, meaning that the attack would require phishing, or otherwise tricking an end user into opening a malicious document. These systems may only be used for reading email or browsing Internet sites at industrial sites with very lax security policies.

**Recommendation: Focus research on internal ICS components which have network protocol exposures.**

---

2. CVSS v3.0 specification: <https://www.first.org/cvss/specification-document>





## Better Update Processes

---

Industrial software is often operated on a segmented network that can be difficult to patch and test, yet the update process for many security issues does not consider this segmentation.

Control systems software is increasingly using integrated version control management. Even when the software update mechanisms require allowing the affected software to connect to the internet and check for updates, the advisories confusingly suggest isolation.

**Recommendation: Vendors should provide a method of locating an update server within a control systems DMZ and provide digitally signed updates.**

Advisories should include software or firmware versions and use product versioning that makes sense. Product versioning in software is generally difficult to navigate, however some product lines contain particularly difficult version strings.

**Recommendation: Provide a date-based versioning scheme or stick to Semantic Versioning.**

Several advisories in 2017 and 2018 listed patches that did not fully remediate the underlying vulnerability. Dragos identified multiple instances of insufficient patching recommendations in 2018, and it is likely this will continue in 2019.

**Recommendation: Affected vendors should develop unit tests or other automated tests for vulnerabilities and ensure that these tests become a part of the quality assurance process for future releases.**

---





## Promote Self-Reporting and Working with Vendors

Vendors self-reporting vulnerabilities is becoming increasingly common, and researchers are willing to engage vendors directly to report some security issues. Likely the stigma in the ICS world against reporting vulnerabilities directly to the vendor, and fear of lawsuits, is diminishing with time.

When a vendor releases an advisory claiming that the vulnerability was discovered in-house, the report tends to have far fewer errors. Only 18% of vendor-produced advisories had errors in the CVSS score, versus 32% overall.

**Recommendation: Vendors should continue to produce and release in-house research.**

When a researcher worked directly with the vendor on an advisory, as opposed to working through an external CERT such as ICS-CERT, the error was also lower, at 24%.

**Recommendation: Researchers should be willing to reach out to vendors as a first step in the vulnerability reporting process.**



# OPERATIONS IMPACT

Dragos assesses each vulnerability's operational impact on industrial control processes. Specifically, threats against industrial processes result in three impact categories: loss of view, loss of control, or both. Where possible, Dragos further clarifies whether a loss of view is known or unknown, and whether a loss of control is hard or soft in vulnerability descriptions.



ICS VULNERABILITY  
IMPACT CATEGORIES



2018 ADVISORIES  
OPERATIONAL  
IMPACT





## ICS Vulnerability Impact Categories

### LOSS OF VIEW

The inability to monitor and/or read the system state

**KNOWN LOSS:** A system no longer displays data due to a communications failure, which should result in an alarm

**UNKNOWN LOSS:** A device or system is displaying data, however the data does not represent the actual measurement

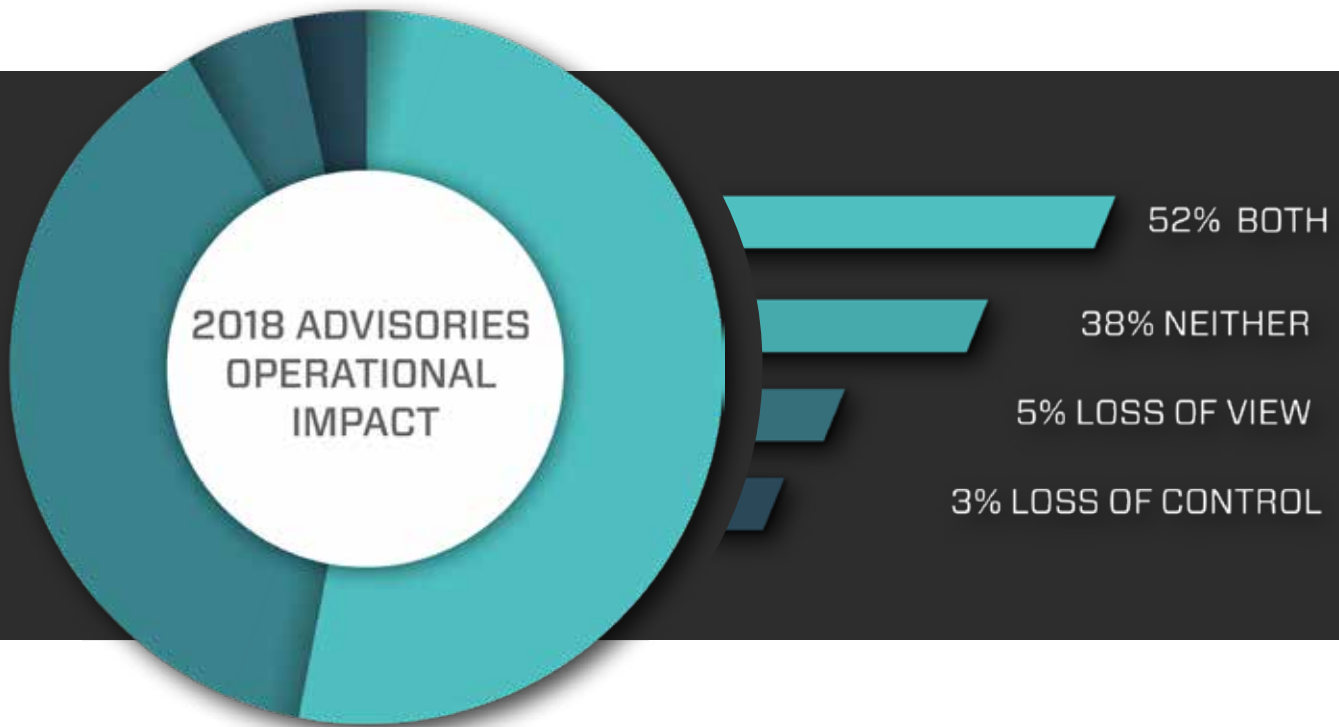
### LOSS OF CONTROL

The inability to modify the system state

**HARD LOSS:** A device is unable to respond to input

**SOFT LOSS:** A device continues to respond to inputs, based on pre-programmed logic, but prevents an operator from intervening





Vulnerabilities which lead to both a loss of view and control occur in the core of traditional control networks affecting both field devices (PLCs, RTUs, etc.) as well as management devices such as human-machine interface (HMI) systems and engineering workstation (EWS) software. This means that over half (60%) of ICS-related vulnerabilities can cause an operations outage, at least for the component affected by the advisory.

**57%** of all total ICS-related vulnerabilities reported in 2018 could result in a loss of view.

**60%** of all total ICS-related vulnerabilities reported in 2018 could cause either loss of view or loss of control, meaning that these could cause a major operations failure.


**55%** of all total ICS-related vulnerabilities reported in 2018 could result in loss of control.



# PERIMETER LIKELIHOOD

Most industrial control networks exist as individual entities separated from the internet by the business or corporate network. Even within an industrial control network, devices are layered –some are close or even inside the business network while others are deep and more inaccessible. Dragos assesses each vulnerability based on the exposed product's usual proximity to the ICS network perimeter: high (close), medium, low, and none (far).

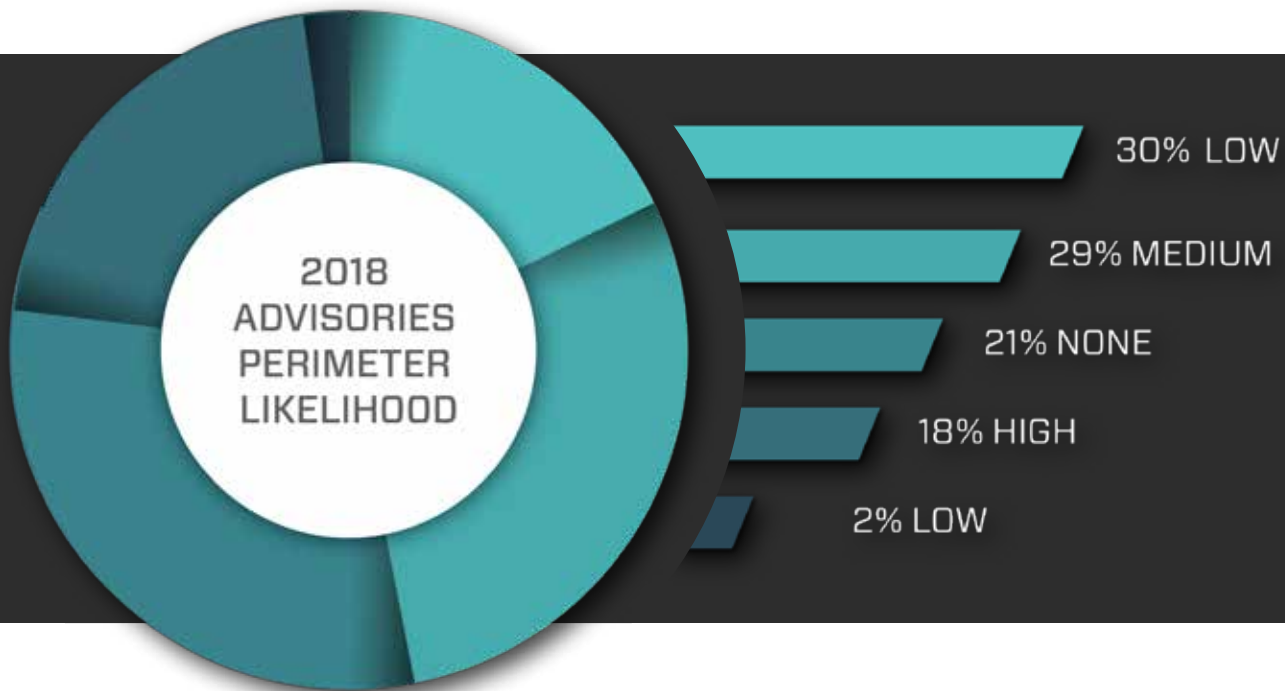
The “Unknown” category includes a chip-level vulnerability and medical device advisory that was incorrectly labeled in 2018.



2018 ADVISORIES  
LIKELIHOOD OF  
ICS BORDER



PERIMETER  
LIKELIHOOD



## PERIMETER LIKELIHOOD

---

**High:** Perimeter-connected or even internet-connected. Directly accessible by a non-ICS network. Examples: historians, OPC servers, firewalls and VPN products, as well as cellular and other external network gateways. These systems will be connected to Level 4 or Level 3 on the Purdue Model.

**Medium:** Network devices which will cross-connect multiple networks and are managed from one of the connected networks. Management will most often occur from the Purdue Level 2, 3, or a special management network. However in some insecure schemes they may be managed from DMZ or even corporate networks. Reconfiguration or poor configuration of these systems may expose ICS networks to business/corporate or internet networks.

**Low:** Central assets on control networks (e.g. HMI, EWS). These map to Purdue Level 2 networks.

**None:** Products and assets generally several steps from another network such as field controllers (e.g. PLCs, RTUs). These map to Purdue Level 1 networks.

---



**80%** of all vulnerabilities affect systems unlikely to be used to pivot into an ICS network.

Perimeter Impact: None through Medium

**18%** of 2018 ICS-related vulnerabilities would be used to gain initial access to control network.

Perimeter Impact: High

**73%** of 2018 ICS vulnerabilities impact interior control systems components.

(HMI, EWS, protocol translators, and process interface systems)

**28%** of all advisories affect either field devices, or industrial equipment.

(industrial-rated network switches, serial to Ethernet converters, programmable logic controllers)

The trends in vulnerability research and advisories have continued largely unchanged from 2017. Researchers continue to spend significant resources identifying vulnerabilities in interior ICS components, with very little work done to secure the important border/perimeter systems.

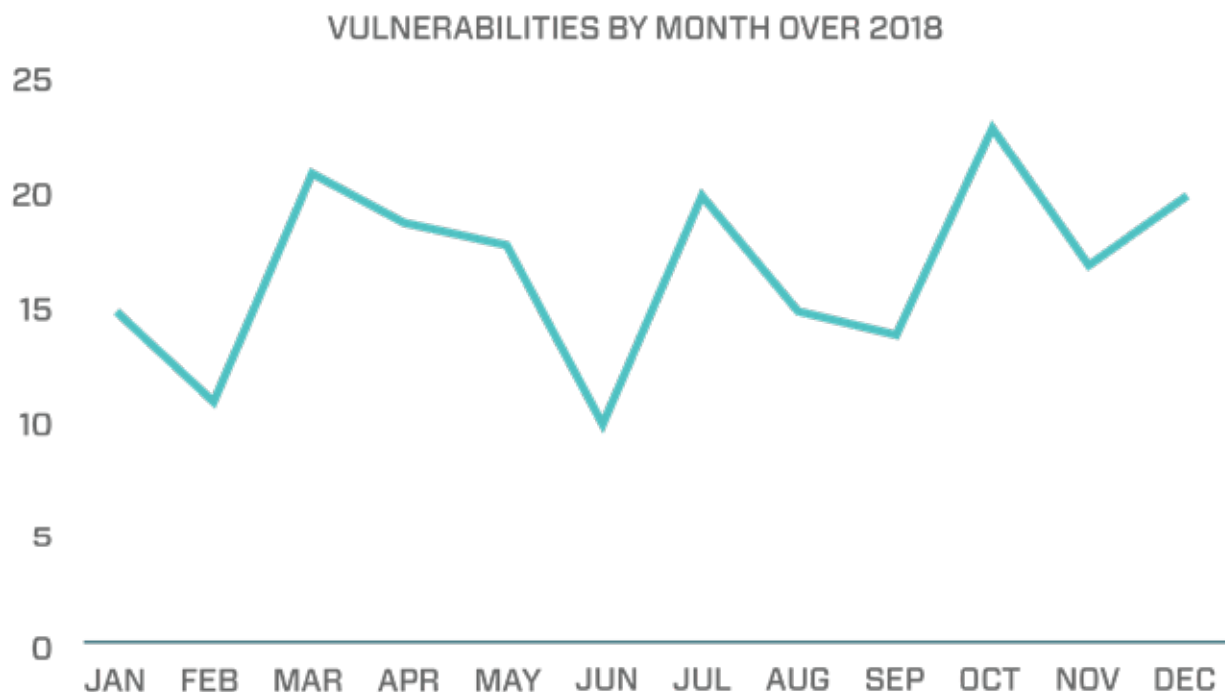
Patching disparity continues to be an issue. Patching, especially patching field devices or industrial network equipment, can be challenging for most operators to perform in a timely manner. Even when patched, most PLCs use insecure-by-design configuration protocols, making actual exploitation of these systems moot. Protocol translators such as serial to Ethernet converters are much the same – even without the ability to reconfigure the device, an attacker can take advantage of the insecure-by-design serial protocol using only the exposed features of such a translator, issuing commands to the serial device without authentication in most cases.

While an attacker may try to take advantage of a protocol translator vulnerability, many of these systems allow unauthenticated configuration changes at a minimum. These configuration changes, both for field devices and for protocol translators, provide an easy avenue for at least denial-of-service – the attacker can easily change a system IP address and deny the owner's ability to communicate.



# VULNERABILITY DISCLOSURES OVER TIME

---



## VULNERABILITY DISCLOSURES OVER TIME

On average, organizations disclosed 17 vulnerabilities each month through 2018, slightly greater than 14 vulnerabilities disclosed monthly in 2017.

Accounting for known conferences, the disclosure rate remained reasonably flat through 2018.

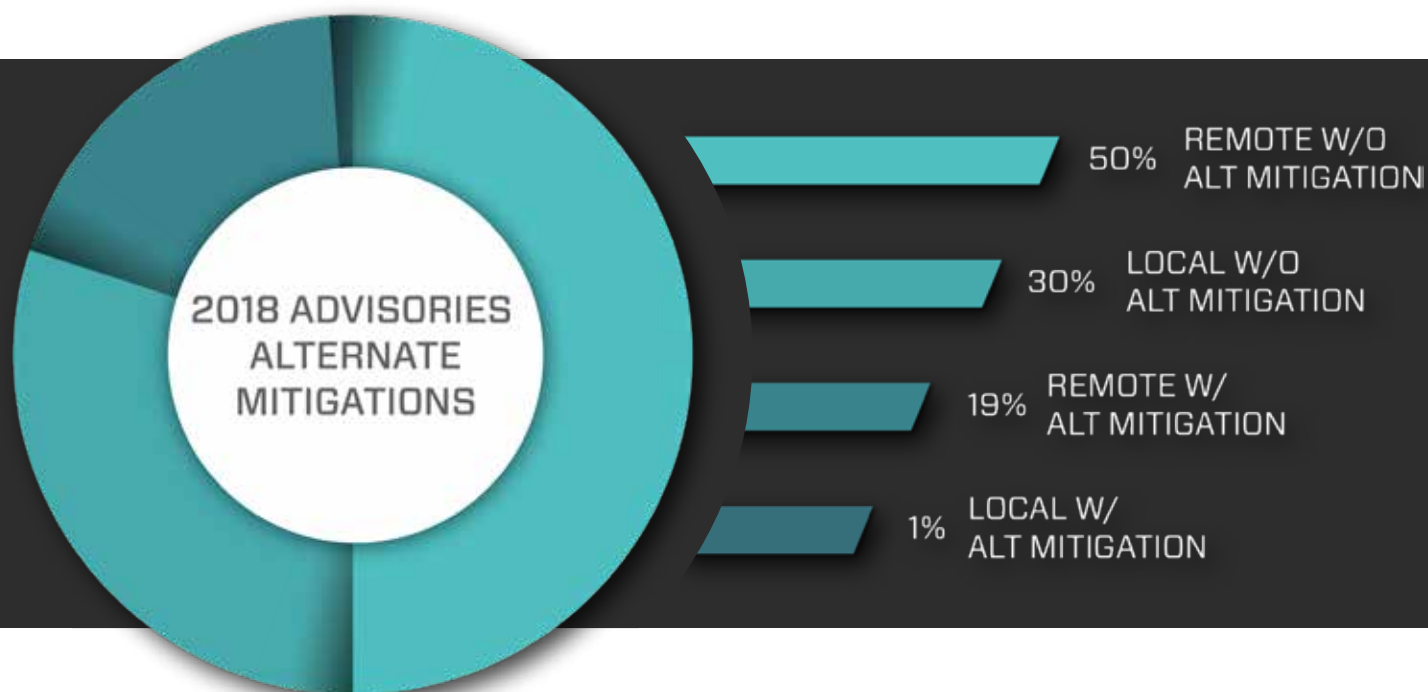
Similar to 2017, a majority of disclosed vulnerabilities map to Purdue Levels 2 & 3.

An increase in ICS-related vulnerability disclosures in July and August most likely coincides with the Black Hat and DEF CON security conferences. This trend was also observed in 2017 – a noticeable spike in advisories in July, with fewer vulnerabilities reported in June and September. The spike in October appears to be coincidental: researchers published several high-profile projects, a number of wide-ranging vulnerabilities were also disclosed in that month, and vendors also self-reported more vulnerabilities in October than on average. Dragos expects the variability in monthly reporting will continue, simply as an artifact of the low volume.





# MITIGATION ADVICE VERSUS EXPLOITABILITY



## MITIGATION ADVICE VERSUS EXPLOITABILITY

Network-exploitable vulnerability advisories still largely lack information on the port or service affected, while few local vulnerabilities suggest even basic information about the issue, such as a file type.

A prime example of a locally-exploitable issue for which a practical alternative mitigation exists is DLL hijacking. End users can, in most cases, enable a Windows configuration option to mitigate this issue in lieu of patching. Yet, of the six DLL hijacking advisories from 2018, none of them contained this useful advice.

**5%** of locally-exploitable vulnerabilities contain some alternative besides "patch"

**28%** of network-exploitable vulnerabilities included port number information with the public advisory

**21%** of vulnerabilities overall had some form of mitigation besides "patch"



# CONCLUSION

---



## CONCLUSION

---

2018 experienced a repeat of many of Dragos' observations from 2017. Researchers still focus on interior controls systems, and advisories continue to lack practical alternate mitigations. 2018 saw an overall 25% increase in vulnerability reporting, focused primarily on HMI systems.

Moving forward, patch management is going to be an area of increased attention, especially with an increasing number of security advisories. As more vendors develop automatic update services, end users will desire automated or semi-automated systems to quickly look up which software versions are installed on process control workstations and servers, as well as quickly determine what versions have security issues. This will likely be driven by compliance. Patch management systems with an ability to locate a repository within a control systems DMZ will also be a likely product offering. With time, advisories will more frequently point to these patch management systems in the mitigation advice.

In 2018 we also saw an increasing trend of vendors self-reporting vulnerabilities, and researchers working with vendors on the coordinated disclosure of security issues. This suggests the ICS community is following the same trend of general software vulnerability disclosure and working in partnership or collaboration directly with vendors.

## METHODS

---

Dragos uses public and private vulnerability sources and produces its own non-public vulnerability discovery and analysis on industrial hardware and software as part of our WorldView threat intelligence product. Dragos independently assessed all vulnerabilities and mitigations and, in many cases, also physically validated them.

Dragos-tracked statistics include advisories published through ICS-CERT, advisories that are published through company product CERTs and PSIRTs, and general IT security advisories that are widely-applicable to the safe operation of a process control network. This last category includes vulnerabilities in commonly-used VPN and firewall systems, as well as vulnerabilities in software that sees regular, and frequently misunderstood, use in control system environments.

---

Dragos began tracking advisory accuracy in 2018. The overall high number of inaccurate reports is a risk – many organizations use public advisory data to either reduce risk or satisfy compliance requirements. Inaccurate advisories mean that these efforts are wasted and that relying upon advisories to prioritize patching or other remediation is not meeting the goal of reducing risk.

CVSS itself is partly to blame. It can be difficult to evenly and accurately apply the scoring system to vulnerabilities, particularly when the specifics of the vulnerability are not made public. Indeed, CVSS itself has hidden assumptions – it is really an exploitability scoring system, not a vulnerability scoring system – and the community's realization of this fact is finally coming to the fore.

2019 holds some promise where vulnerability reporting is concerned. The year began with the first open discussion about reinventing CVSS to focus on industrial factors at the 2019 S4 Conference. It is doubtful that such a system will reach wide adoption in 2019, however the community may start to coalesce on a standard for reporting ICS vulnerabilities using a domain-specific description.