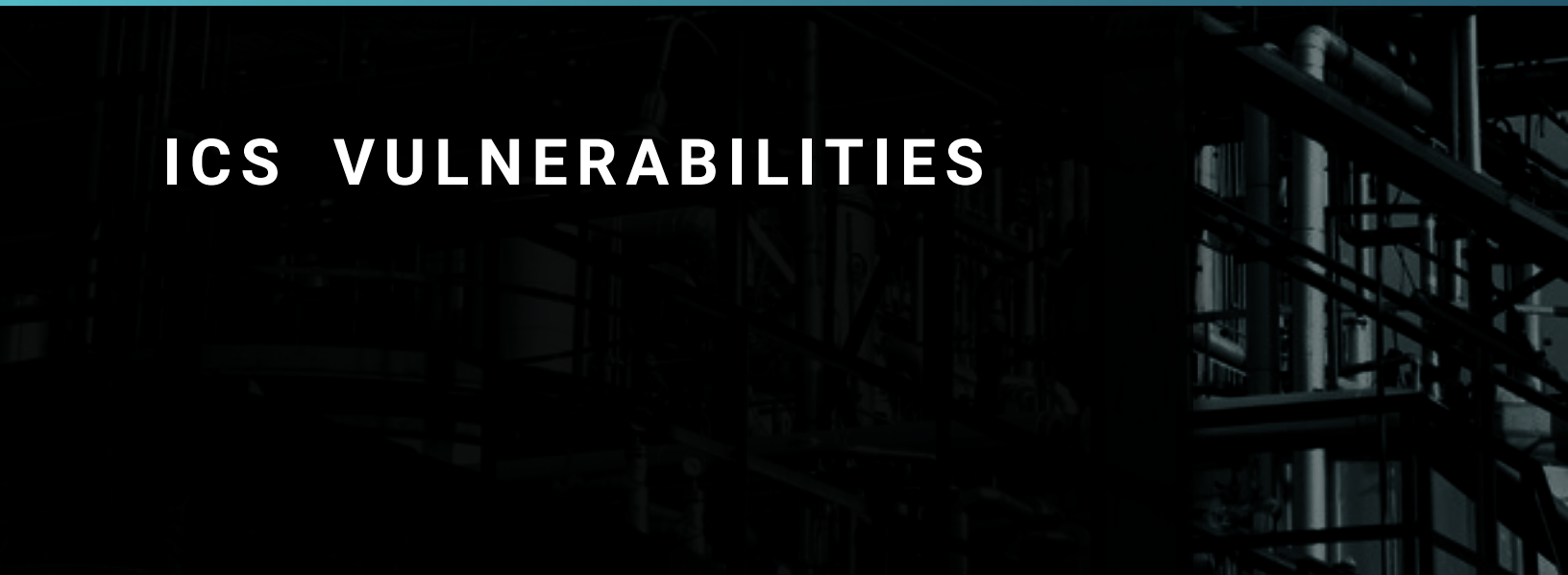
DRAGOS

2019

YEAR IN REVIEW



ICS VULNERABILITIES

CONTENT

INTRODUCTION

DRAGOS VULNERABILITY ANALYSTS ASSESSED 438 INDUSTRIAL CONTROL SYSTEM (ICS) VULNERABILITIES REPORTED BY A VARIETY OF SOURCES INCLUDING INDEPENDENT RESEARCHERS, VENDORS, AND ICS-CERT.

The findings in this report are a comprehensive look at ICS vulnerability statistics, including how they affect industrial control networks and whether appropriate mitigation is provided alongside the published advisories.

Dragos identifies errors in the vulnerability scores associated with public reports, a critical part of our vulnerability assessments. By identifying and updating errors in vulnerability scores, Dragos vulnerability assessments help asset owners and operators better prioritize and manage patching and update procedures.

Additionally, Dragos threat intelligence provides updated vulnerability assessments that include scoring corrections, additional mitigations, and advice for end-users going further than published advisories.

2019

KEY FINDINGS

77% of assessed vulnerabilities were considered "deep within" a control systems network, requiring some existing access to a control systems network to exploit.

9% of advisories applied to products generally associated with systems bordering the enterprise, which could facilitate initial access into operations.

26% of advisories had no patch available when the initial advisory came out, presenting a challenge for users trying to take action on the published vulnerability.

30% of advisories published incorrect data preventing operators from accurately prioritizing patch management.

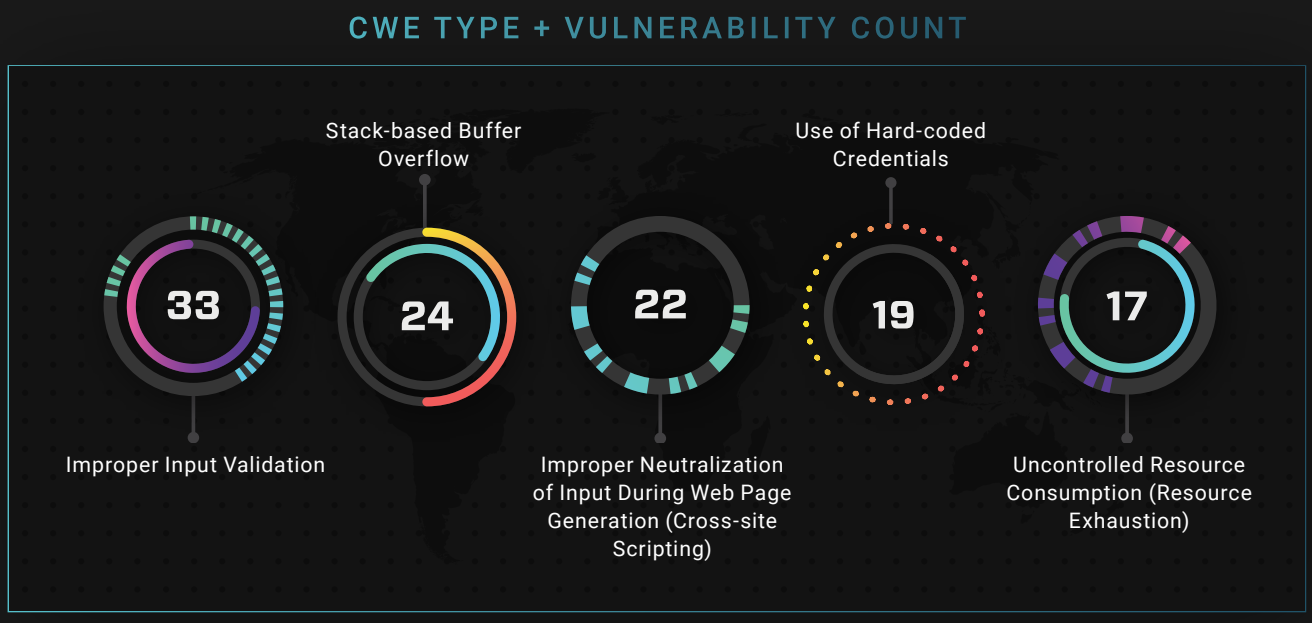
40% of advisories applied to engineering workstation and operator station software requiring user interaction, or internet connectivity, to exploit, which may be rare and difficult depending on the industry.

VULNERABILITIES

OVERVIEW

In 2019, Dragos assessed and validated or corrected 212 vulnerability advisories, comprising 438 total vulnerabilities with each individual vulnerability having its own identification known as a CVE identifier.

DRAGOS CATEGORIZES VULNERABILITIES BY TYPE AS DESIGNATED BY THE COMMON WEAKNESS ENUMERATION (CWE) LIST.[1] THE FOLLOWING LIST IS THE TOP FIVE CWES COVERED IN 2019 OUT OF 116 UNIQUE VULNERABILITY TYPES.



1 https://cwe.mitre.org/

ANALYST NOTE

Dragos primarily monitors advisories published through ICS-CERT, but also evaluates security advisories in products not covered by ICS-CERT.

In 2019, Dragos tracked just five advisories from other sources, including virtual private network (VPN) appliances which are commonly used in industrial settings, as well as third-party software that is commonly used for web applications and workstation security in industrial environments.

OF THE ADVISORIES ASSESSED IN 2019, 77% EXIST "DEEP WITHIN" A CONTROL SYSTEMS NETWORK.

This means the vulnerabilities only affect products that belong on engineering workstations, human machine interface (HMI) systems, operator panels, industrial network equipment, and field devices themselves. To exploit these vulnerabilities, an adversary would require existing access to the operations network.

Only 9% of advisories applied to products that are generally associated with border systems, including data historians, OPC servers, cross-domain web applications, and VPN services that are likely to be exposed to corporate networks on a well-architected control system. Such vulnerabilities could potentially facilitate an adversary to cross the IT/OT boundary and gain initial access to operations networks.

The remaining vulnerabilities fit into neither category. These include systems such as door access controls, video management systems, and heating, ventilation, and air conditioning (HVAC) controllers, which generally have no direct impact on operations or are not industrial-specific. However, adversaries previously exploited HVAC contractor connections

to obtain initial access to building control networks and could be used as an initial access vector.

Network-exploitable issues accounted for 74% of all advisories in 2019, while the remainder required some level of existing or physical access to exploit. Network-exploitable vulnerabilities generally do not require an adversary to be logged-in to a workstation in order to exploit but do require some level of network access to the target system.

VULNERABILITY METRICS

FOR CONTROL SYSTEMS

CONTROL SYSTEMS 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.

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 displays data, however the data does not represent the actual measurement.

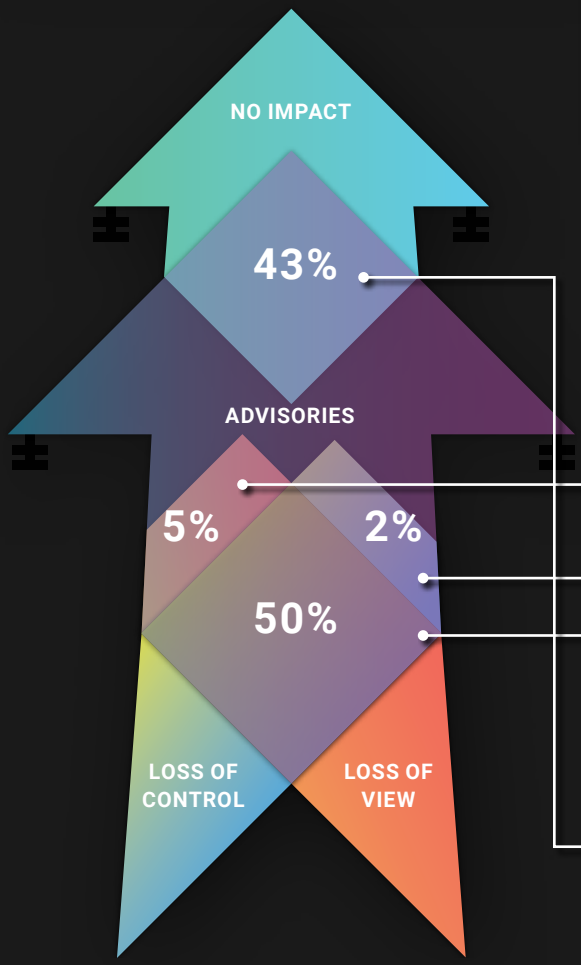
In 2019, Dragos analysts identified a high degree of overlap between Loss of View and Loss of Control impacts in advisories.

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.



5% of advisories could only cause a loss of view (but no loss of control) via exploitation

2% of advisories could result in a loss of control (but no loss of view)

50% of advisories could cause both a loss of view and a loss of control

43% of advisories could cause neither impact directly

EXPOSURE 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.

9% of advisories covered products that would be deemed high-likelihood initial targets in the ICS space. These include data historians, OPC servers, VPN services, and other cross-domain services that are regularly exposed to at least some set of corporate servers or workstations. Such devices can serve as initial access vectors to the operations network.

40% of advisories covered engineering workstation and operator station software. An adversary could exploit these vulnerabilities by persuading a user to interact with a malicious file, or by gaining access to the vulnerable device via the internet. Note: such devices should not be connected to the internet, but it is not uncommon to see services such as email on an engineering workstation.

37% of advisories covered field equipment: industrial controllers, sensors, and the network equipment responsible for connecting controllers and sensors to the broader control systems network. While the majority of industrial controllers are still insecure by design, vulnerabilities in the industrial network equipment can disrupt process automation in a manner that is difficult to not only troubleshoot but to recover from. In most cases, an attacker would require virtual or physical access to the device in order to exploit vulnerabilities in field equipment.

MITIGATION ADVICE

26% of advisories had no patch available when the initial advisory came out. Additionally, 76% of the advisories which had no patch offered and no practical alternative mitigation advice at all in the advisory. This means an end user cannot take action based on the advisory alone.

55% of advisories had a patch, but no alternate mitigation.

In 77% of all of the advisories which provided no alternate mitigation, Dragos provided alternate mitigation advice that could be used to reduce risk in lieu of patching. This included providing protocol details suitable for restricting communications to the vulnerable service, file extensions to monitor on incoming email and web proxies, and other local system or group policy configurations that could reduce the risk of or impact from exploitation.

67% of advisories for ICS-specific or proprietary network protocols included an alternate mitigation in the advisory. Vendors are still somewhat reluctant to announce what port or service is associated with a bug, although this seems to be improving with time.

ERROR RATES

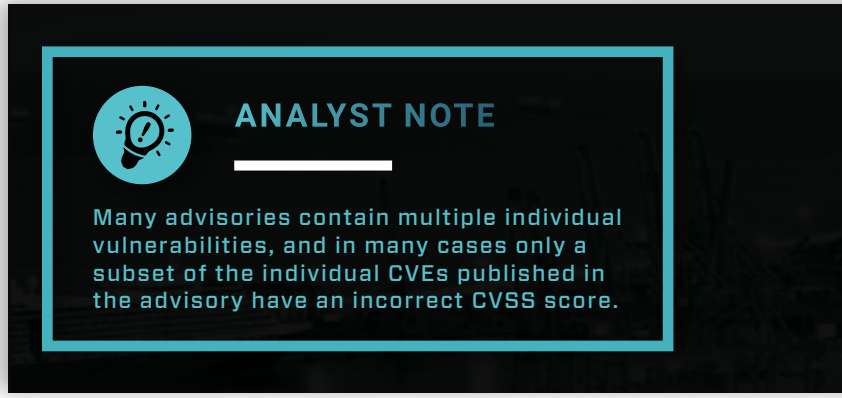
VULNERABILITIES ARE SCORED BASED ON THE CRITICAL VULNERABILITY SCORING SYSTEM (CVSS).

A vulnerability's severity is determined based on a variety of factors including the attack vector and attack complexity, and privileges or user interaction required to exploit the vulnerability. Eight variables make up the "Base Score." The total sum of the eight variables make up the severity score, which is designed to be an easy-to-read numeric assessment of the vulnerability. Companies often prioritize patching based on the CVSS score – the more severe a vulnerability, the more attention may be paid to it.

In 2019, Dragos began tracking advisory errors with a great deal of granularity, putting an increased focus on this important data point. Dragos found that vulnerabilities frequently contain an incorrect severity score, which can potentially harm security and patching prioritization at affected companies. When our analysts identify a score that is incorrect, we update and publish the correct score for our threat intelligence customers.

ERROR RATE RESULTS

Overall in 2019, **30%** of advisories published incorrect data, and **19%** of individual CVEs contained errors. This represents a massive improvement over 2018, which had a **32%** error rate for individual CVEs. However, this still represents a significant error rate, and shows that advisories can often mislead practitioners who hope to use these scores to triage mitigation.



Of the errors identified in 2019, Dragos found **73%** to be more severe than the public advisory revealed, **26%** to be less severe, and **1%** to have an identical numeric score but a different exploitation vector.

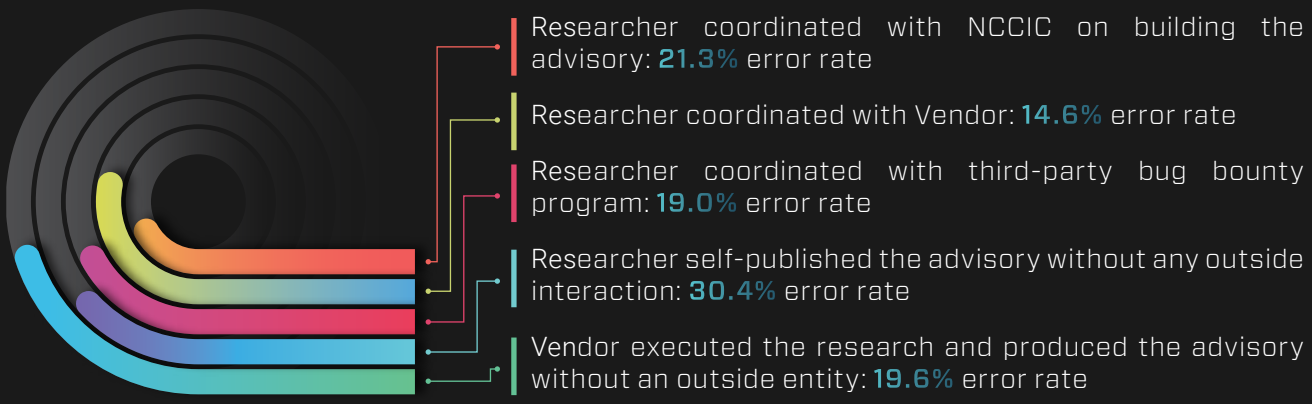
The most common errors in CVSS scores include Scope and User Interaction requirements:

- Many cross-site scripting (XSS) bugs are not properly labeled as having Scope changed in spite of this being a specific example used in the CVSS standard.
- Many cross-site request forgery (CSRF) bugs and file format vulnerabilities are not marked with a User Interaction requirement.
- Finally, Confidentiality and Availability scores are often marked incorrectly for vulnerabilities which textually describe arbitrary code execution or denial of service as an impact.

In 2019, very few CVEs contained errors in the very basic Attack Vector metric this year, signifying another positive improvement to CVE scoring. For example, in 2018, public advisories marked many advisories as Network Exploitable when they were not related to any network service, and vice-versa. Several advisories in 2018 marked routable protocols as only Adjacent Network exploitable or only Locally exploitable. This metric, more than anything, can help end users triage vulnerabilities. Dragos analysts are pleased to see these errors shrink over time.

IN 2018 DRAGOS OBSERVED THAT VENDOR-PRODUCED ADVISORIES CONTAINED A MUCH LOWER ERROR RATE THAN ADVISORIES FROM OTHER SOURCES.

This trend continued in 2019. As in 2018, the most accurate reporting in 2019 occurred when researchers reported vulnerabilities directly to the vendor. Error rates for each reporting category are listed below. Error percentages are rated as per individual CVE, not per advisory:



This once again demonstrates vendors collaborating with third-party researchers results in the most accurate vulnerability reporting.

It is worth mentioning that third-party bug bounty program coordination saw a massive improvement over 2018 (which had an error rate above 50%). The majority of bug bounty errors occurred early in 2019, suggesting that coordination with these programs may end up providing the best information in the future.

FREE AND DEMO SOFTWARE

JUST 25% OF ADVISORIES COVER SOFTWARE WITH A FREE OR DEMO VERSION THAT IS READILY AVAILABLE.

A common misperception is that ICS-related security issues are more frequently discovered in "free" ICS software packages which may not represent the software and hardware actually used in plants. While more vendors offer demo or free restricted-use licenses for their enterprise software, the majority of vulnerability advisories still cover software for which there are no demo or free versions, and hardware or other specialty industrial equipment which cannot be tested legally without the researcher making some initial investment.

RECOMMENDATIONS

FOR DEFENDERS

THE MAJORITY OF NETWORK-EXPLOITABLE SECURITY ISSUES COVER JUST A HANDFUL OF PROTOCOLS.

For industrial-specific protocols, end users are best served by restricting access to interior components on TCP/102, TCP/502, TCP/4840, Ports 44818 and 2222, and TCP/11740+UDP/1740.

Monitoring a network for suspicious behaviors is always extremely helpful. ICS protocols tend to be insecure by design and may allow for malicious operations which technically use no exploit. After patching systems which use the services above, an end user may still be vulnerable to malicious operations, and should monitor their control systems network for suspicious commands:

- Typically "write" or "assert output" style commands, especially from non-HMI systems, and
- Engineering/programming commands which originate outside of typical hours and from workstations which are not normally used for such a purpose.

On the IT protocol side, HTTP (TCP/80 and TCP/443), SNMP (UDP/161), and Telnet and SSH (TCP/23 and TCP/22) represent the largest vulnerable surfaces. In many cases, vulnerabilities in these services can result in a loss of operational view or control, especially when the services are exposed by field equipment such as PLCs and network switches, or HMI systems.

FOR VENDORS

PUBLISHING ALTERNATE MITIGATION GUIDANCE IN THE PUBLIC ADVISORY SHOULD BE A PRIORITY FOR BOTH VENDORS AND ICS-CERT.

Declining to provide the information in the public advisory offers very little in terms of preventing adversary exploitation and hurts defenders who may lack the resources or skills to investigate software.