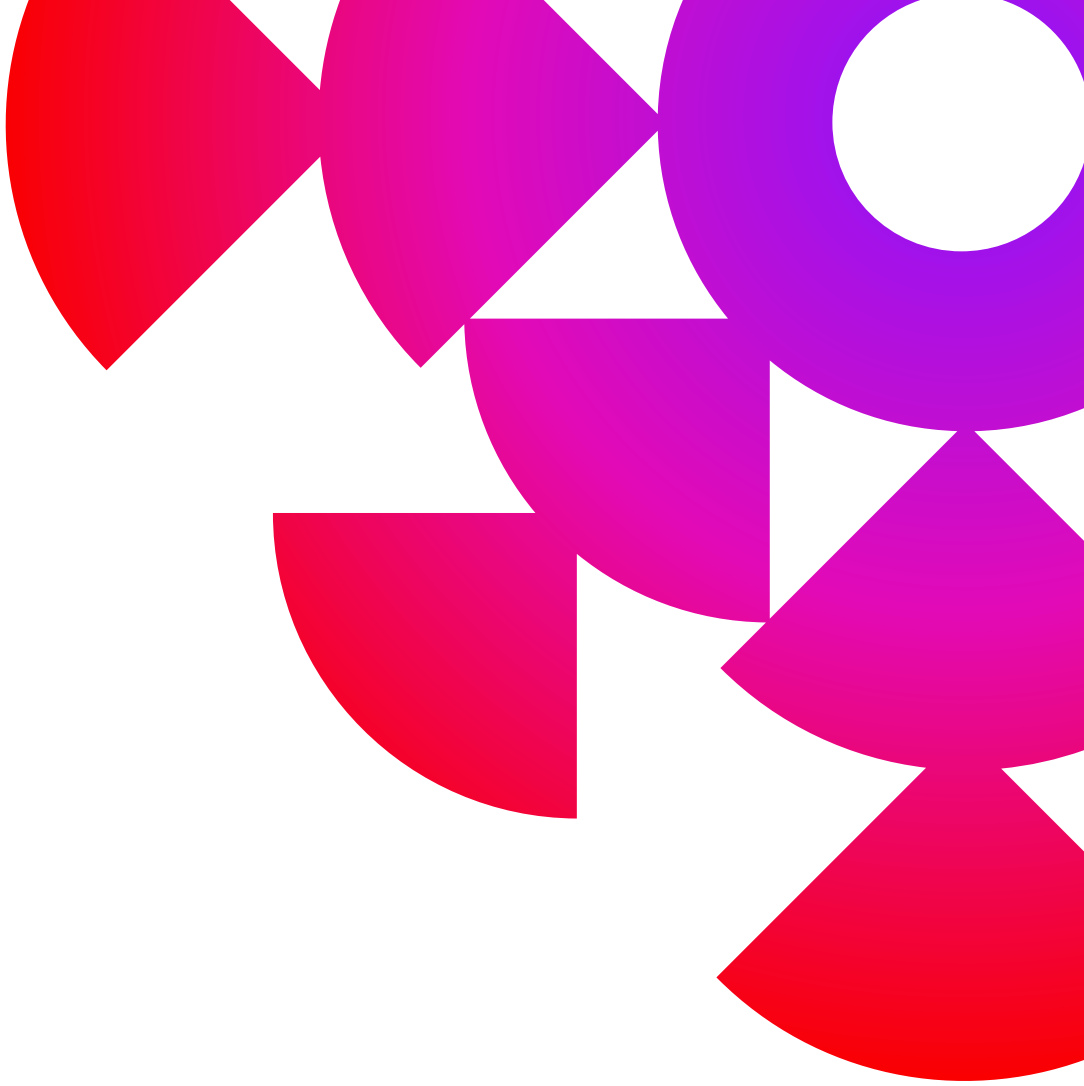


CLAROTY BIANNUAL ICS RISK & VULNERABILITY REPORT: 1H 2020

CLAROTY

CONTENTS

EXECUTIVE SUMMARY

The inaugural Claroty Biannual ICS Risk & Vulnerability Report details The Claroty Research Team's assessment of industrial control system (ICS) vulnerabilities disclosed publicly in the first half of 2020 (1H 2020). These vulnerabilities include those discovered by The Claroty Research Team and those discovered by other researchers and organizations.

The objective of this report is to provide nuanced insight into the ICS risk and vulnerability landscape, the challenges it poses to operational technology (OT) security practitioners, and what conclusions can be drawn from publicly available data. It is important to note that security incidents that involved ICS vulnerabilities disclosed in 1H 2020 are not a focal point of this report because such incidents—whether ICS-targeted or opportunistic attacks—can skew perceptions of the true prevalence and impact of a given vulnerability.

Key findings of this report include:

- During 1H 2020, the National Vulnerability Database (NVD) disclosed 365 vulnerabilities that affected ICS products from 53 vendors. More than 75% of those vulnerabilities were assigned high or critical Common Vulnerability Scoring System (CVSS) scores.

- Vulnerabilities in ICS products disclosed during 1H 2020 are most prevalent in the energy, critical manufacturing, and water & wastewater sectors—all of which are designated as critical infrastructure sectors.

- More than 70% of the vulnerabilities disclosed during 1H 2020 can be exploited remotely via a network attack vector. This observation reinforces the fact that fully air-gapped OT networks that are fully isolated from cyber threats have become exceedingly uncommon, highlighting the critical importance of protecting internet-facing ICS devices and remote access connections. The rapid shift to a remote workforce—and thus the increased reliance on remote access connections to OT networks—due to the COVID-19 pandemic further underscores this point and exacerbates the associated risks.

- The top five most prevalent security weaknesses, or Common Weakness Enumerations (CWEs), manifested in the ICS vulnerabilities disclosed during 1H 2020 are all ranked highly on The MITRE Corporation's 2019 CWE Top 25 Most Dangerous Software Errors list due their relative ease of exploitation and potential impacts.

- The number of ICS vulnerabilities disclosed in 1H 2020 increased by roughly 10% compared to 1H 2019. While it may seem logical to assume that this and similar increases were caused by an increase in adversary activity and/or a decrease in ICS vendors' security posture, the primary factors are likely heightened awareness of the risks posed by ICS vulnerabilities and increased focus from researchers and vendors on identifying and remediating such vulnerabilities as effectively and efficiently as possible.

ABOUT THE CLAROTY RESEARCH TEAM

The Claroty Research Team is an award-winning group of OT security researchers known widely for its development of proprietary OT threat signatures, OT protocol analysis, and discovery and disclosure of ICS vulnerabilities. Fiercely committed to strengthening OT security and equipped with the industry's most extensive ICS testing lab, the team works closely with leading industrial automation vendors to evaluate the security of their products.

The Claroty Research Team is an award-winning group of OT security researchers known widely for its development of proprietary OT threat signatures, OT protocol analysis, and discovery and disclosure of ICS vulnerabilities.

To date, the team has discovered and disclosed more than 44 ICS vulnerabilities—26 of which were disclosed in 1H 2020 alone.

Recognizing the critical need to understand the ICS risk and vulnerability landscape in its entirety and how the vulnerabilities discovered by Claroty researchers fit into that landscape, The Claroty Research Team created an automated collection and analysis tool that ingests ICS vulnerability data from trusted open sources including the NVD and the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

The outputs of this tool shed light on key trends and contextualized implications pertaining to ICS vulnerabilities, the risks they pose to OT networks, and their variations across different vendors, products, geographies, time periods, criticality scores, and impacts, among other attributes. These outputs are the foundation of the research and analysis throughout this report.

PART 1: ASSESSMENT OF ICS VULNERABILITIES DISCOVERED BY CLAROTY & DISCLOSED IN 1H 2020

The 26 ICS vulnerabilities discovered by The Claroty Research Team that were disclosed during 1H 2020 are largely representative of the direction and core objectives of the team's research.

Always seeking to provide the greatest benefit to the OT security community, the team prioritizes research focused on ICS vendors and products with vast install bases, those that play integral roles in industrial operations, and those that utilize protocols or have other characteristics in which the team has considerable expertise. The team also prioritizes critical or otherwise high-risk vulnerabilities that could be exploited to compromise the availability, reliability, and/or safety of industrial operations.

1.1. AFFECTED ICS VENDORS

A breakdown of the 11 ICS vendors of the products affected by the 26 vulnerabilities discovered by Claroty and disclosed in 1H 2020 is as follows. The majority of these vendors' affected products are widely deployed across sectors globally, a key factor in The Claroty's Research Team's decision to focus on them.

AFFECTED ICS VENDORS

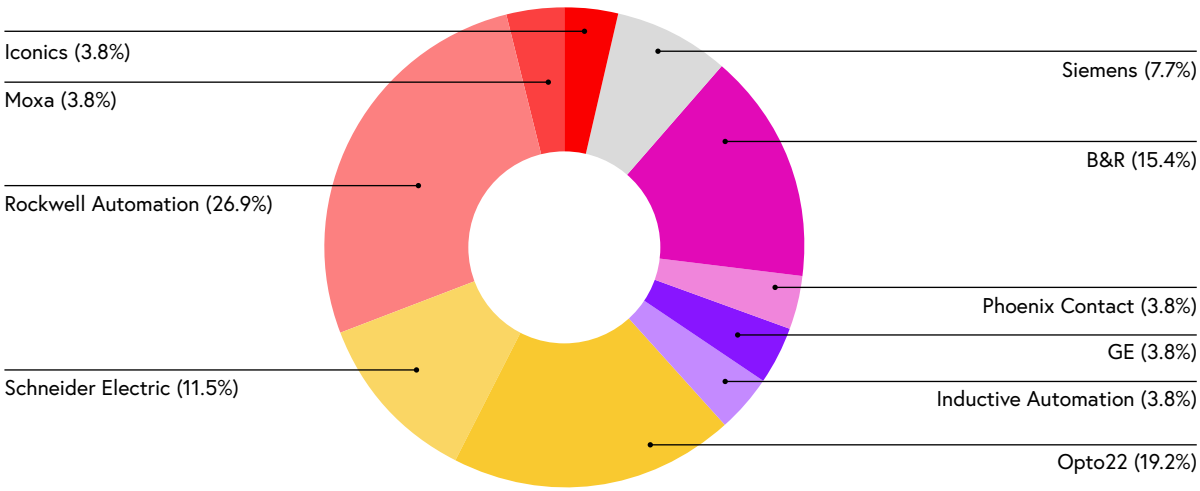


Figure 1.1: Breakdown of Claroty-discovered vulnerabilities by affected vendors

1.2. AFFECTED ICS PRODUCT TYPES

Engineering workstations (EWS) and programmable logic controllers (PLCs) comprise the majority of the ICS products affected by the 26 vulnerabilities discovered by The Claroty Research Team and disclosed in 1H 2020. The team focuses its research efforts heavily on these product types because they play crucial roles in industrial operations and thus tend to be highly appealing targets for adversaries.

Engineering workstations (EWS) and programmable logic controllers (PLCs) comprise the majority of the ICS products affected by the 26 vulnerabilities discovered by The Claroty Research Team and disclosed in 1H 2020.

Specifically, EWS often have some degree of connectivity to the IT network. They also have access to the shop floor and the PLCs that control physical processes within OT networks. For adversaries seeking to manipulate or compromise those physical processes, gaining access to an EWS provides an initial foothold. EWS are also generally considered to be prone to vulnerabilities, which—when combined with their tendency to have IT connectivity—can cause adversaries to perceive them as both desirable and viable targets.

EWS are also generally considered to be prone to vulnerabilities, which—when combined with their tendency to have IT connectivity—can cause adversaries to perceive them as both desirable and viable targets.

A full breakdown of the ICS product types affected by the 26 vulnerabilities discovered by The Claroty Research Team and disclosed in 1H 2020 is as follows:

AFFECTED ICS PRODUCT TYPES

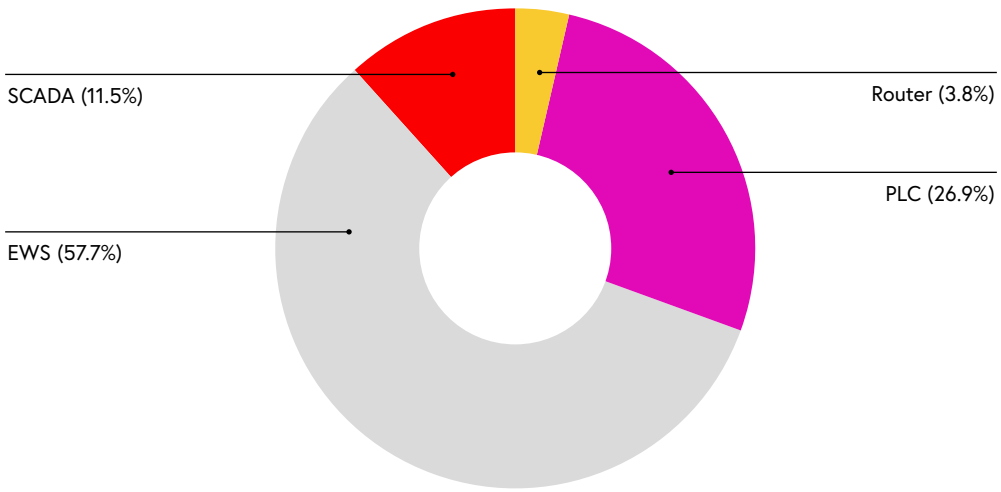


Figure 1.2: Breakdown of Claroty-discovered vulnerabilities by affected product type

1.3. VULNERABILITY IMPACT TYPES

Successful exploitation of any of the 26 vulnerabilities discovered by The Claroty Research Team and disclosed in 1H 2020 could have serious impacts on affected OT networks, with more than 60% of the vulnerabilities enabling some form of remote code execution (RCE). Other impact types covered by these 26 vulnerabilities include denial-of-service (DoS) and power-over-ethernet (PoE).

More than 60% of the vulnerabilities enable some form of remote code execution (RCE).

IMPACT CLASS

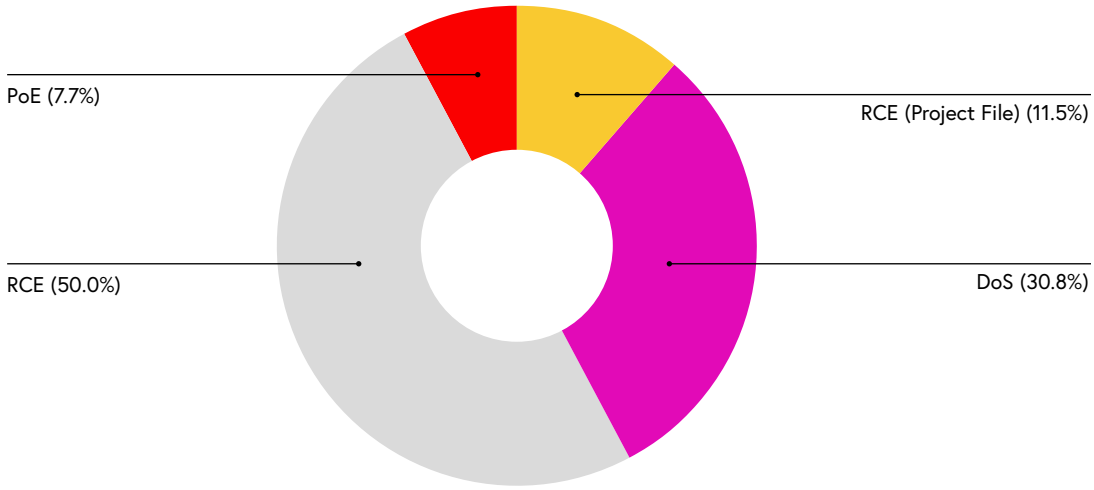


Figure 1.3: Breakdown of Claroty-discovered vulnerabilities by impact class

PART 2: ASSESSMENT OF ALL ICS VULNERABILITIES DISCLOSED IN 1H 2020

This section of the report provides a statistical and contextual assessment of all ICS vulnerabilities published in 1H 2020. These vulnerabilities include the 26 discovered by The Claroty Research Team, in addition to all others discovered and publicly disclosed by other researchers, vendors, and organizations within the same time period.

2.1. TOTAL COUNT OF ICS VULNERABILITIES AND ADVISORIES

ICS Vulnerabilities Disclosed by the NVD in 1H 2020
The NVD published 365 ICS vulnerabilities during 1H 2020, reflecting a 10.3% year-over-year increase compared to the 331 published in 1H 2019. Over 75% of these vulnerabilities were assigned high or critical CVSS severity ratings. This observation reflects the broader tendency among ICS security researchers to focus on identifying vulnerabilities with the greatest potential impact in order to maximize harm reduction.

The NVD published 365 ICS vulnerabilities during 1H 2020, reflecting a 10.3% year-over-year increase compared to the 331 published during 1H 2019.

VULNERABILITIES PUBLISHED

365

Total ICS Vulnerabilities Published by the NVD

VENDORS AFFECTED

53

Total Vendors Affected by ICS Vulnerabilities

CVSS SEVERITY RATINGS OF NVD-PUBLISHED VULNERABILITIES

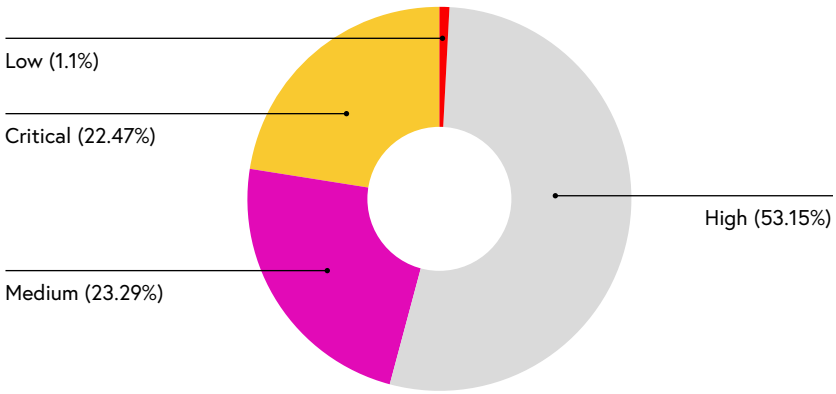


Figure 2.1a: Breakdown of the total count of ICS vulnerabilities published by the NVD in 1H 2020

Advisories Issued by ICS-CERT in 1H 2020

ICS-CERT published 139 ICS advisories during 1H 2020, a 32.4% increase from the 105 published during 1H 2019. The advisories included 385 common vulnerabilities and exposures (CVEs) affecting 53 vendors.

Security researchers—including those affiliated with ICS vendors or other organizations—account for 71.4% of ICS-CERT advisories issued during 1H 2020, attesting to the critical role of third parties in vetting the security of the ICS devices and systems that underpin industrial operations.

The remaining 28.6% of advisories originated from in-house research and testing conducted by ICS vendors. This constitutes a modest but notable increase from the 21.6% of ICS-CERT advisories originating from vendors during 1H 2019, which may reflect increased scrutiny among ICS vendors on the security of their products.

ADVISORIES ISSUED

139

Total ICS Security Advisories Issued by ICS-CERT

VENDORS AFFECTED

53

Total Vendors Affected by ICS Security Advisories Issued by ICS-CERT

ORIGINS OF DISCOVERIES INCLUDED IN ICS-CERT ADVISORIES

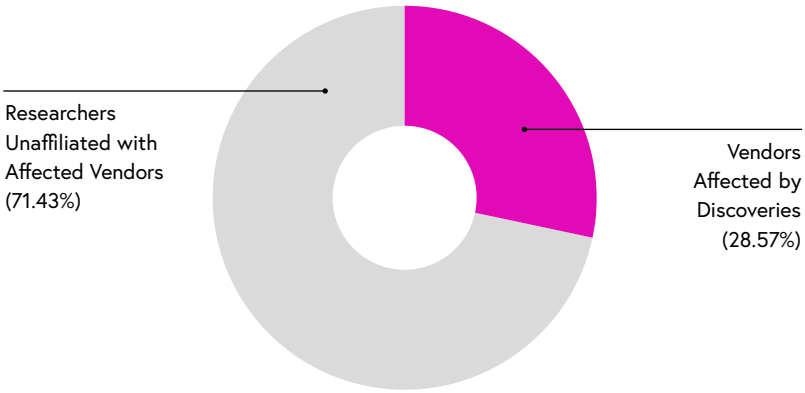


Figure 2.1b: Breakdown of the total count of ICS security advisories issued by ICS-CERT in 1H 2020

Monthly Comparison of ICS Vulnerabilities Disclosed in 1H 2020

The 10% increase in the number of ICS vulnerabilities published by the NVD in 1H 2020 compared to 1H 2019 can largely be accounted for by a significant spike in the number of vulnerabilities published during March and April 2020. In May 2020, however, the NVD published less than one-third the number of vulnerabilities it had published in May 2019.

MONTHLY COMPARISON OF ICS VULNERABILITIES PUBLISHED BY THE NVD

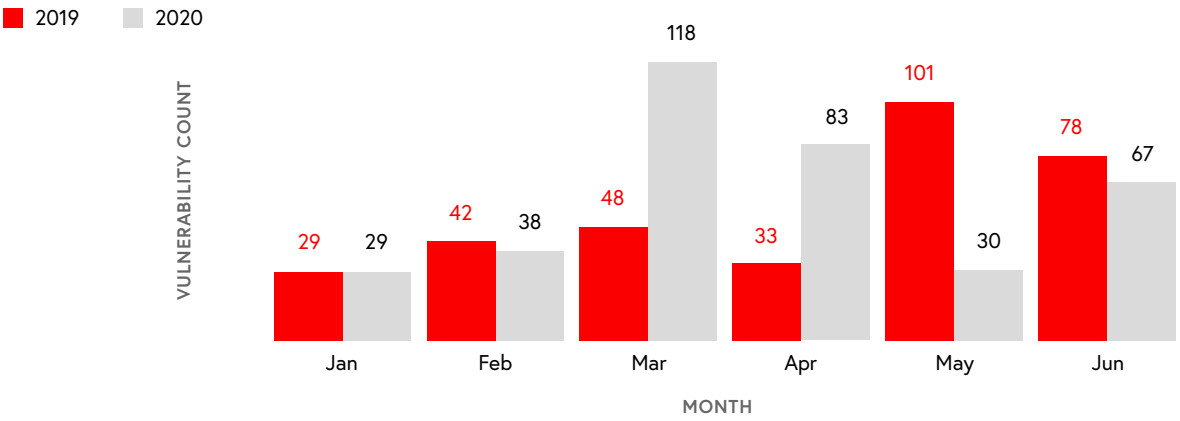


Figure 2.1c: Comparison of the total number of ICS vulnerabilities published by the NVD during each month of 1H 2019 and 1H 2020

A month-by-month comparison of the total number of CVEs included in ICS-CERT advisories issued during 1H 2019 and 1H 2020 shows a significant number of CVEs included in advisories issued during the months of February and March 2020, followed by a spike in June.

While 385 unique CVEs were included in ICS-CERT advisories in 1H 2020, the total number of CVEs included in such advisories is 400 because certain CVEs were included in multiple advisories. Some ICS-CERT advisories issued in 1H 2020 also included CVEs that were assigned in previous years but had since been updated to reflect newly surfaced information.

MONTHLY COMPARISON OF ADVISORIES ISSUED BY ICS-CERT

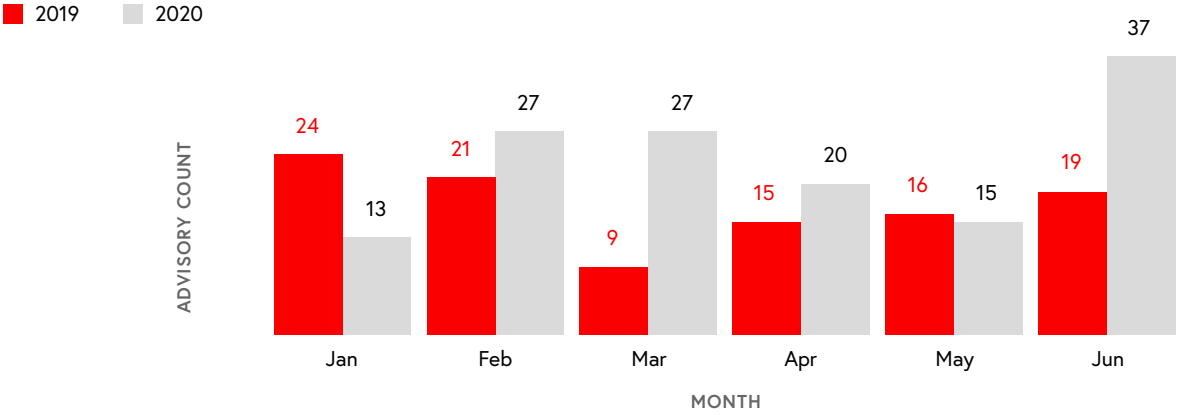


Figure 2.1d: Comparison of the total number of ICS security advisories issued by ICS-CERT during each month of 1H 2019 and 1H 2020

2.2. AFFECTED ICS VENDORS

ICS Vendors Affected by Vulnerabilities Published by the NVD in 1H 2020
The 365 ICS vulnerabilities disclosed by the NVD in 1H 2020 affected products from 53 vendors. ICS automation vendor Moxa led the pack with 39 out of the total 365 vulnerabilities affecting its products, trailed closely by ABB, Siemens, Wago, and Schneider Electric.

ICS automation vendor Moxa led the pack with 39 out of the total 365 vulnerabilities affecting its products, trailed closely by ABB, Siemens, Wago, and Schneider Electric.

TOP FIVE VENDORS AFFECTED BY VULNERABILITIES PUBLISHED BY THE NVD

Figure 2.2a: Breakdown of vendors affected by the greatest number of ICS vulnerabilities published by the NVD during 1H 2020

Vendors Affected by ICS-CERT Advisories During 1H 2020

Meanwhile, out of the 139 advisories issued by ICS-CERT during 1H 2020, 37 pertained to Siemens products, by far the most of any vendor mentioned in such advisories. Coming in a distant second was Rockwell Automation, which had products affected by nine ICS-CERT advisories during that same period.

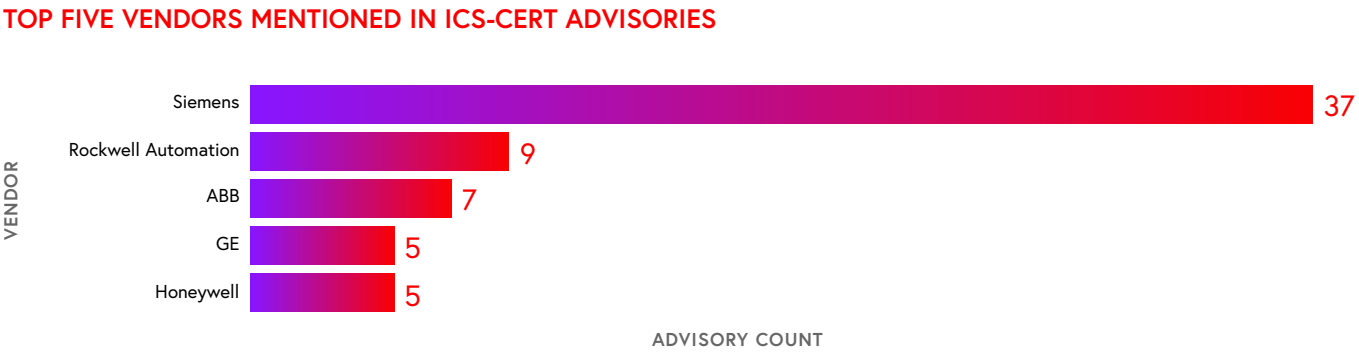


Figure 2.2b: Breakdown of top five affected vendors mentioned in ICS-CERT advisories during 1H 2020

ICS Vendors Affected by Vulnerabilities Disclosed in 2020 1H but not in 2019

During 1H 2020, 21 vendors whose products had not been affected by any ICS vulnerabilities disclosed in 2019 were affected by at least one ICS vulnerability disclosed in 1H 2020. Eight of these vendors specialize in industrial automation and four specialize in medical technologies.

During 1H 2020, 21 vendors whose products had not been affected by any ICS vulnerabilities disclosed in 2019 were affected by at least one ICS vulnerability disclosed in 1H 2020.

VENDOR	PRIMARY INDUSTRY
AutomationDirect	Industrial Automation
B&R Automation	
ICONICS	
KUKA	
SAE IT Systems	
Synergy Systems & Solutions (SSS)	
Systech Corporation	
VISAM	
Baxter	Medical
BIOTRONIK	
Insulet	
Spacelabs	
Fazecast	ICS Software
Triangle Microworks	
Auto-Maskin	Oil & Gas, Marine
ENEA	Telecommunications
Hirschmann	Automation & Control
IP Infusion	Networking
ITRON	Energy & Water Resource Management
Sensormatic Electronics	Electronics Manufacturing
SWARCO Traffic Systems	Traffic Engineering

Figure 2.2c: Vendors affected by at least one ICS vulnerability disclosed in 1H 2020 after not being affected by any ICS vulnerabilities disclosed in 2019

It is crucial to recognize that being affected by a significant number of disclosed vulnerabilities does not necessarily signify that a vendor has poor security posture or limited research capabilities. A vendor that allocates ample resources to testing the security of its products is likely to discover more vulnerabilities in them than a vendor that neglects to scrutinize its products to the same extent. The age, catalogue, and install base of each vendor also tend to influence the number of disclosed vulnerabilities affecting its products.

It is crucial to recognize that being affected by a significant number of disclosed vulnerabilities does not necessarily signify that a vendor has poor security posture or limited research capabilities.

2.3. GEOGRAPHIC SCOPE OF AFFECTED ICS PRODUCTS & VENDORS

Install Base of Products Affected by ICS-CERT Advisories in 1H 2020

The overwhelming majority (81.8%) of ICS-CERT advisories issued during 1H 2020 pertained to ICS products deployed worldwide. Meanwhile, 7.0% of advisories pertained to products deployed exclusively in the United States, and 4.7% to products exclusive to Europe.

The overwhelming majority (81.8%) of ICS-CERT advisories issued during 1H 2020 pertained to ICS products deployed worldwide.

DEPLOYMENT OF AFFECTED PRODUCTS

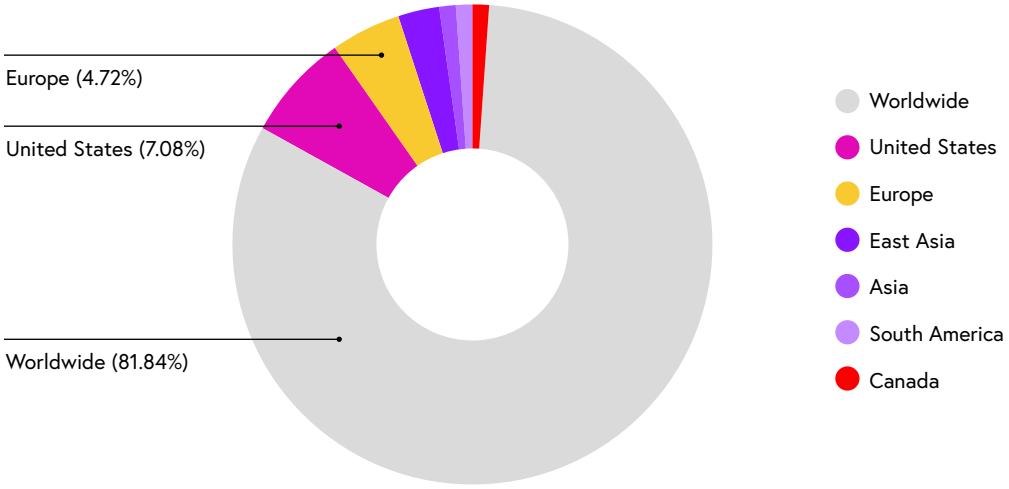


Figure 2.3a: Breakdown of 1H 2020 ICS-CERT advisories by the affected products' geographic scope of deployment

2.4. IMPACT OF ICS VULNERABILITIES BY INFRASTRUCTURE SECTOR

Infrastructure Sectors Affected by ICS-CERT Advisories in 1H 2020

The energy, critical manufacturing, and water & wastewater infrastructure sectors were by far the most impacted by vulnerabilities included in ICS-CERT advisories during 1H 2020. Compared to 1H 2019, the water & wastewater sector experienced a 122.1% increase in ICS-CERT vulnerabilities, while the critical manufacturing and energy sectors respectively experienced 87.3% and 58.9% increases.

ICS-CERT published one vulnerability in 1H 2020 impacting the nuclear reactors, materials, & waste sector, which was not affected by any vulnerabilities disclosed during either half of 2019.

The energy, critical manufacturing, and water & wastewater infrastructure sectors were by far the most impacted by vulnerabilities published in ICS-CERT advisories

VULNERABILITY COUNT BY INFRASTRUCTURE SECTOR

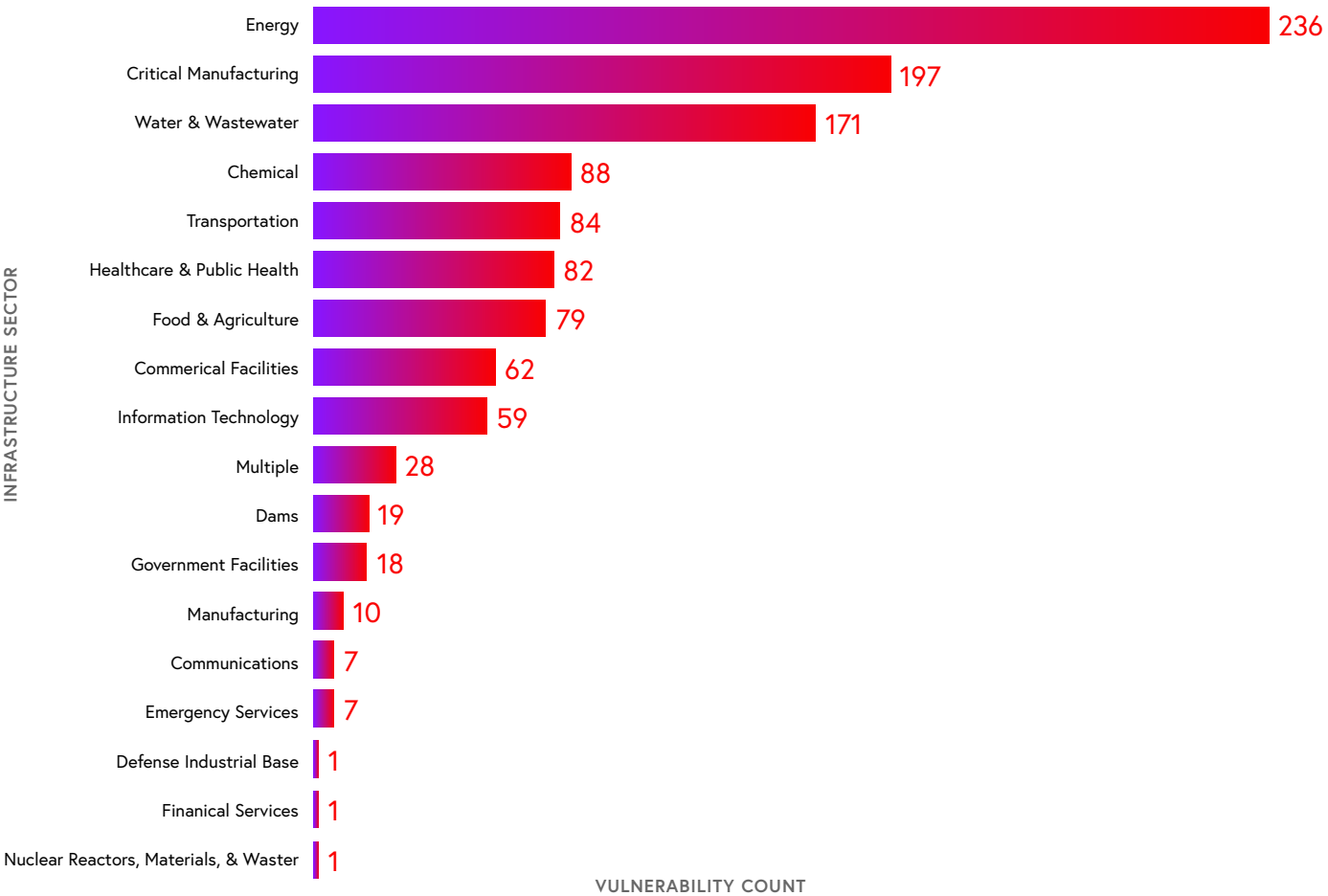


Figure 2.4a: Breakdown of infrastructure sectors affected by vulnerabilities included in ICS-CERT advisories during 1H 2020

YEAR-OVER-YEAR COMPARISON OF VULNERABILITY COUNT BY INFRASTRUCTURE SECTOR

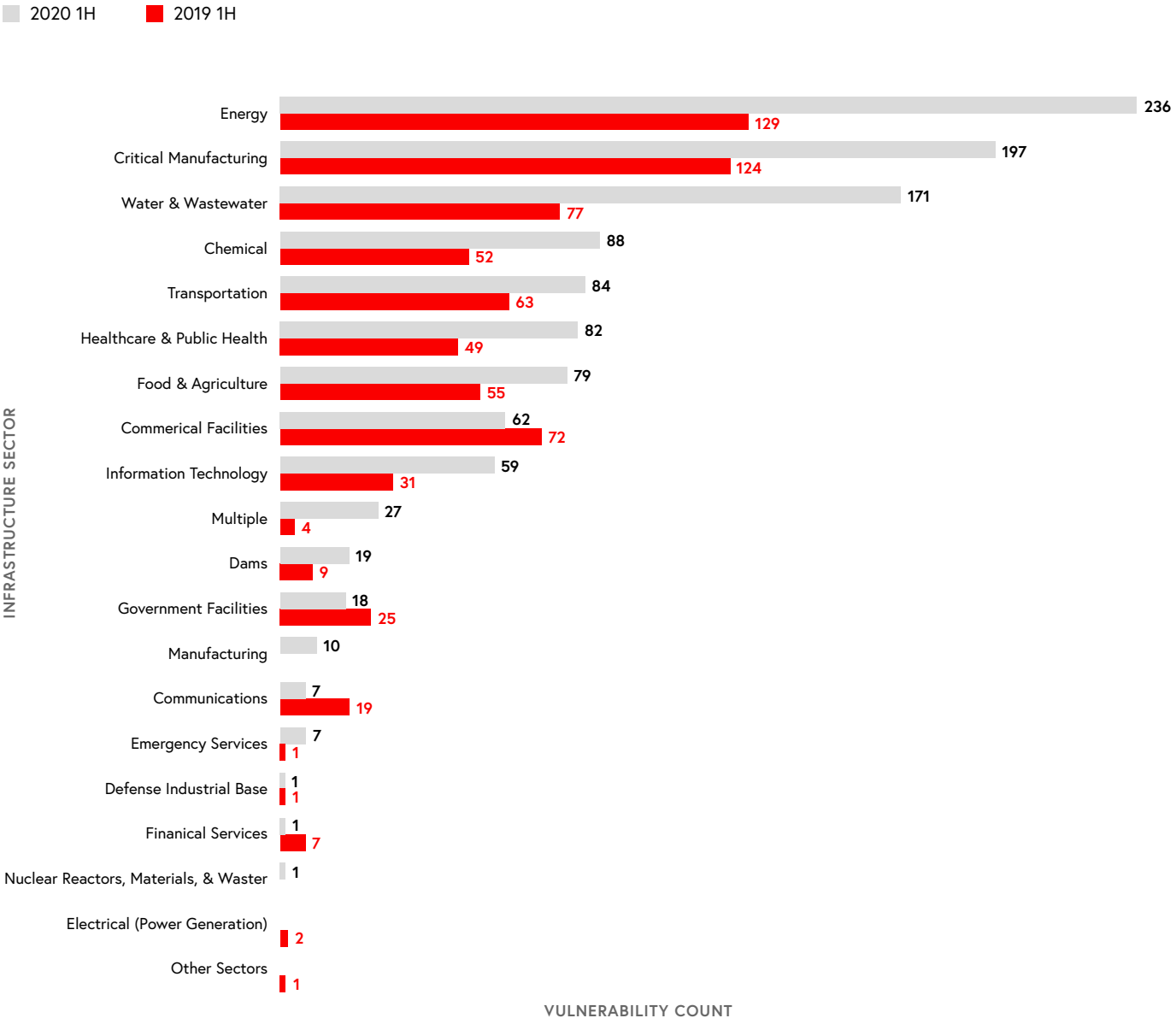


Figure 2.4b: Comparison of the total number of vulnerabilities included in ICS-CERT advisories affecting each infrastructure sector in 1H 2019 and 1H 2020

A monthly breakdown of ICS-CERT vulnerabilities indicates that the energy, critical manufacturing, and water & wastewater sectors were affected by multiple vulnerabilities disclosed during every month of 1H 2020.

MONTHLY COMPARISON OF VULNERABILITY COUNT BY INFRASTRUCTURE SECTOR

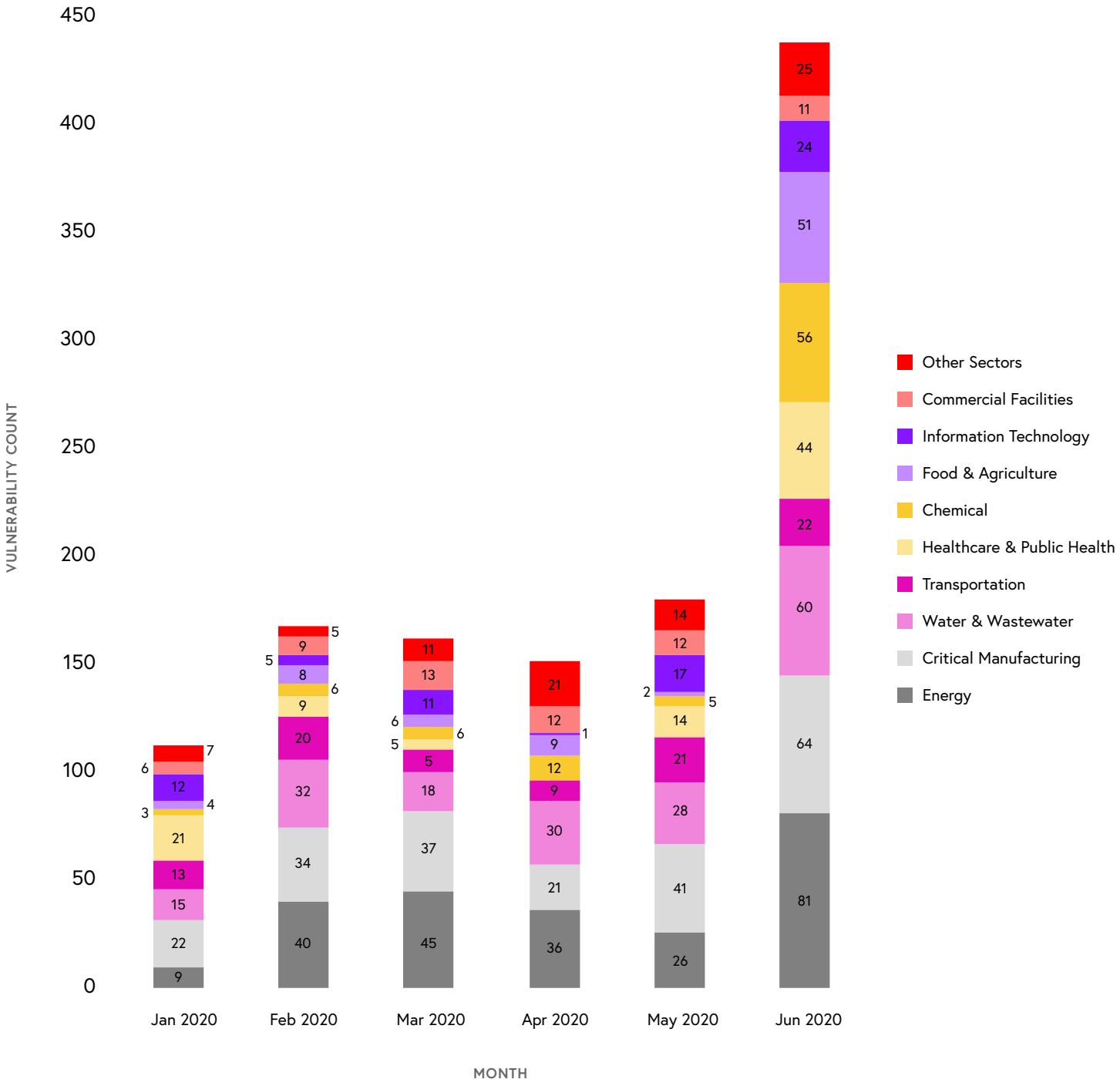


Figure 2.4c: Monthly breakdown of the number of vulnerabilities affecting each infrastructure sector during 1H 2020

2.5. ICS VULNERABILITIES BY ATTACK VECTOR

Attack Vector Distribution of ICS Vulnerabilities Published by the NVD in 1H 2020
More than 70% of the 365 ICS vulnerabilities published by the NVD during 1H 2020 can be exploited remotely via a network attack vector. This observation reinforces the fact that fully air-gapped ICS networks that are completely isolated from cyber threats have become exceedingly uncommon, highlighting the importance of protecting internet-facing ICS devices and remote connections.

Fully air-gapped ICS networks that are completely isolated from cyber threats have become exceedingly uncommon, highlighting the importance of protecting internet-facing ICS devices and remote connections.

The rapid shift to a remote workforce—and thus the increased reliance on remote access connections to ICS networks—due to the COVID-19 pandemic further underscores this point and exacerbates the associated risks.

Aside from the prevalence of network attack vectors, it is also noteworthy that the share of ICS vulnerabilities exploitable via local attack vectors increased from 13.9% during 1H 2019 to 22.5% during 1H 2020. Exploitation of local attack vectors relies on user interaction by another person to perform actions required to exploit these vulnerabilities. These situations are typically where social engineering techniques such as those utilized in phishing attacks come into play; awareness and protection against them is critical.

Exploitation of local attack vectors relies on user interaction by another person to perform actions required to exploit these vulnerabilities.

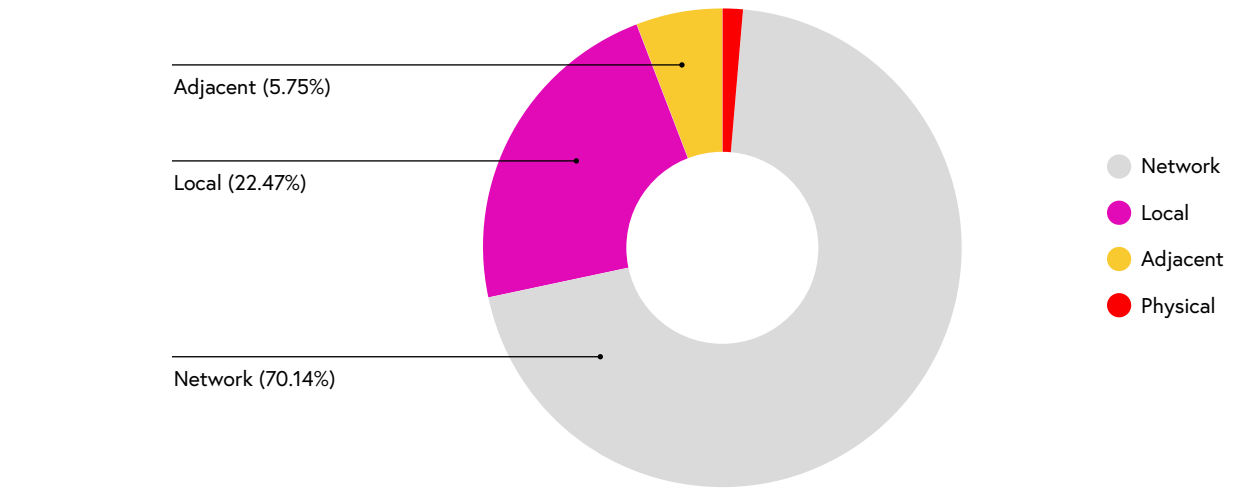


Figure 2.5: Breakdown of ICS vulnerabilities published by the NVD in 1H 2020 by attack vector

2.6. ICS VULNERABILITIES BY CVSS SCORE

CVSS Considerations

The extent to which the CVSS is relevant to OT security remains widely debated, largely because the scoring system was initially developed to quantify the criticality of vulnerabilities present in information technology (IT) networks—not OT networks.

As such, the CVSS is based on the information security principle of the CIA triad, which comprises confidentiality, integrity, and availability. Though technically relevant to any type of network, the CIA triad does not encompass what are arguably the two most important risk variables for OT networks: reliability and safety. This means that the CVSS doesn't fully account for the potential impacts of ICS vulnerabilities that can be exploited to cause physical harm.

Though technically relevant to any type of network, the CIA triad does not encompass what are arguably the two most important risk variables for OT networks: reliability and safety.

Average CVSS Score per Affected ICS Vendor

The following graph shows the average CVSS score for each vendor of affected ICS products, most of which have an average score above seven. This is largely explained by the fact that nearly every vendor had products affected by vulnerabilities that could be exploited to enable unauthorized code/command execution or DoS.

AVERAGE CVSS SCORE PER VENDOR

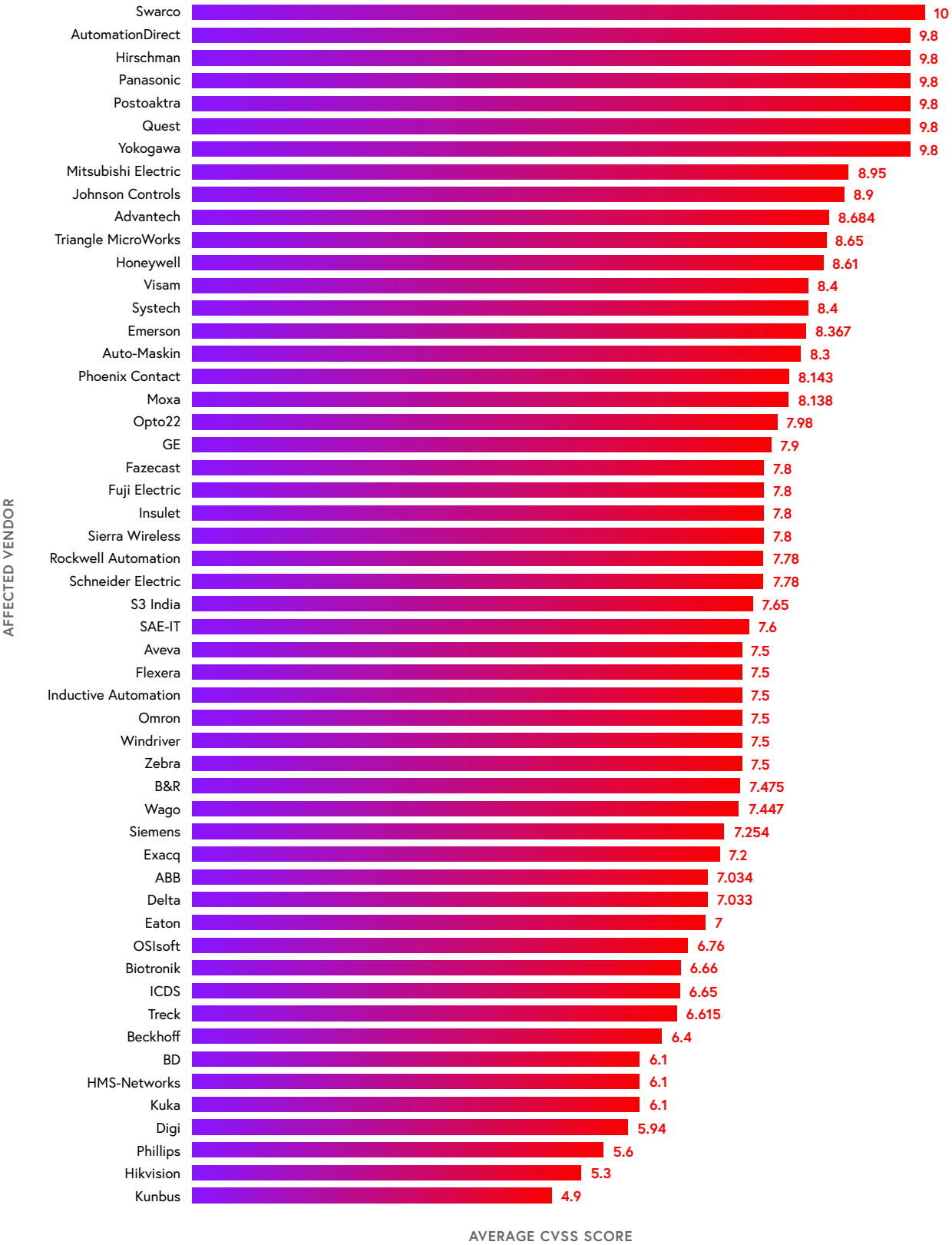


Figure 2.6a: Breakdown of affected ICS vendors by average CVSS score of vulnerabilities published by the NVD during 1H 2020

VULNERABILITY COUNT BY CVSS SEVERY RATING FOR THE TOP 10 VENDORS

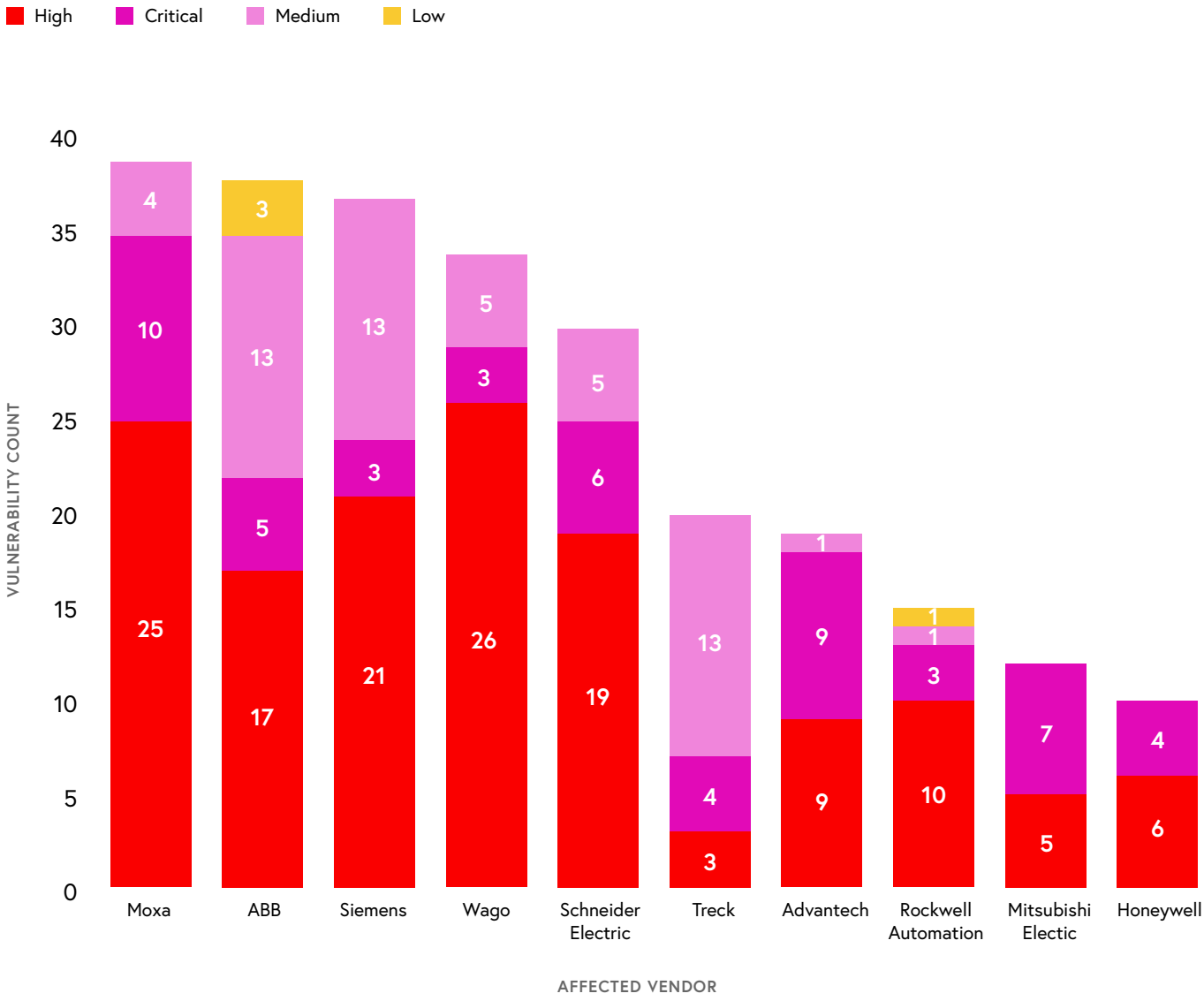


Figure 2.6b: Breakdown of ICS vulnerabilities published by the NVD in 1H 2020 by CVSS severity rating for the top 10 vendors

2.7. ICS VULNERABILITIES BY CWE

Most Prevalent CWEs Manifested in ICS Vulnerabilities Disclosed by the NVD in 1H 2020
The security weaknesses, or Common Weakness Enumerations (CWEs), manifested in the ICS vulnerabilities disclosed by the NVD during 1H 2020 help explain why most of these vulnerabilities have CVSS scores categorized as either high or critical.

Indeed, the top five most prevalent CWEs are all ranked highly on The MITRE Corporation's 2019 CWE Top 25 Most Dangerous Software Errors list due their relative ease of exploitation and ability to enable adversaries to inflict serious damage.

These CWEs include:

1. CWE-787 Out-of-bounds Write
The software writes data past the end, or before the beginning, of the intended buffer. This usually occurs when the pointer or its index is incremented or decremented to a position beyond the buffers' bounds or when pointer arithmetic results in a position outside of a valid memory location.

Successful exploitation can result in data corruption, DoS, or code execution.

- This CWE manifests in **6.78%** of the vulnerabilities, up from 1.36% in 1H 2019.
- This CWE is #12 on MITRE's 2019 Top 25 most dangerous software errors.

2. CWE-20 Improper Input Validation
The product incorrectly validates or does not validate input that may affect the control flow or data flow of the program. A software that validates input improperly allows an attacker to craft the input in a way that is unexpected to the rest of the software.

Successful exploitation can result in control flow alterations, memory modification, DoS, or code execution.

- This CWE manifests in **6.54%** of the vulnerabilities, down from 8.97% in 1H 2019.
- This CWE is #3 on MITRE's 2019 Top 25 most dangerous software errors.

3. CWE-79 Improper Neutralization of Input During Web Page Generation
The software incorrectly neutralizes or does not neutralize user controllable input before it is placed in an output used as a web page which is served to other users.

Successful exploitation can result in code or command execution, bypass of protection mechanisms, or ability to read application data.

- This CWE manifests in **5.08%** of the vulnerabilities, up from 0.51% in 1H 2019.
- This CWE is #2 on MITRE's 2019 Top 25 most dangerous software errors.

4. CWE-78 Improper Neutralization of Special Elements used in an OS Command
The software constructs all or part of an operating system (OS) command using an externally influenced input from an upstream component and incorrectly neutralizes or does not neutralize special elements that could modify the intended OS command when it is sent to a downstream component.

Successful exploitation can result in code or command execution, DoS, file or directory modification, application data modification, ability to read files or directories, ability to read application data, and ability to hide activities.

- This CWE manifests in **4.84%** of the vulnerabilities, down from 7.34% in 1H 2019.
- This CWE is #11 on MITRE's 2019 Top 25 most dangerous software errors.

5. CWE-22 Improper Limitation of a Pathname to a Restricted Directory (Path Traversal)
The software uses external input to construct a pathname that will be used to identify a file or directory that is located underneath a restricted parent directory, and the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory.

Successful exploitation can result in code or command execution, DoS, file or directory modification, and ability to read files or directories.

- This CWE manifests in **4.84%** of the vulnerabilities, up from 1.36% in 1H 2019.
- This CWE is #10 on MITRE's 2019 Top 25 most dangerous software errors.

2.8. POTENTIAL IMPACTS OF ICS VULNERABILITIES

The chart below depicts the most prevalent potential impacts of ICS vulnerabilities published by the NVD during 1H 2020 based on CWE, reflecting the prominence of remote code execution as the leading area of focus within the OT security research community. Behind remote code execution is a clear second tier of potential impacts: allowing an adversary to read application data, cause DoS, or bypass protection mechanisms.

Behind remote code execution is a clear second tier of potential impacts: allowing an adversary to read application data, cause DoS, or bypass protection mechanisms.

VULNERABILITY COUNT BY IMPACT

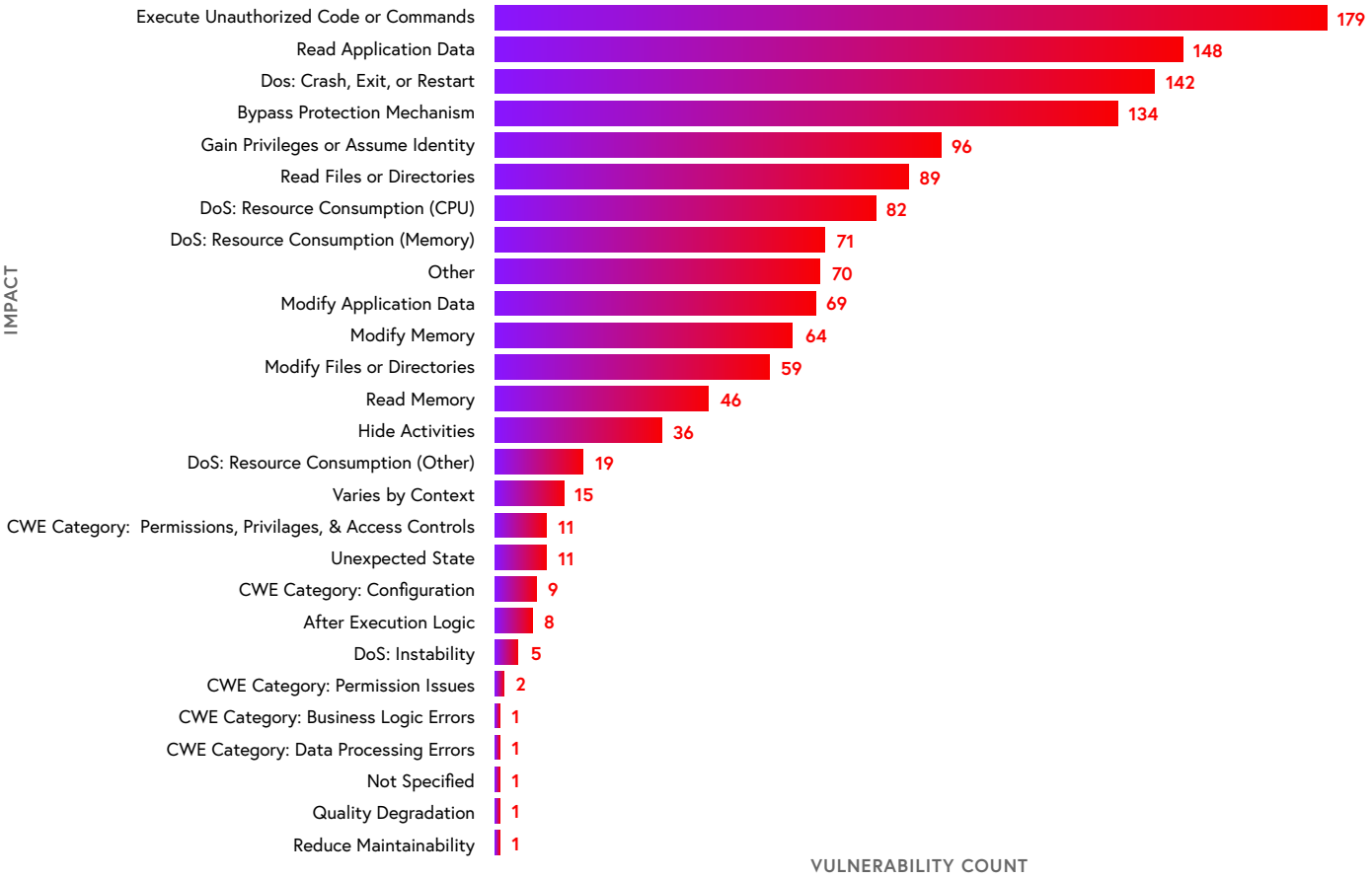


Figure 2.8a: Most prevalent potential impacts of ICS vulnerabilities published by the NVD during 1H 2020

The following graph illustrates the distribution of vendors affected by vulnerabilities that can be exploited to enable unauthorized code/command execution and/or DoS. Most of these vendors have products affected by vulnerabilities that can be exploited to enable one or both of these impacts, which helps explain why the average CVSS score per vendor is above seven.

COUNT PER VENDOR OF ICS VULNERABILITIES WITH CODE/COMMAND EXECUTION AND DOS IMPACTS

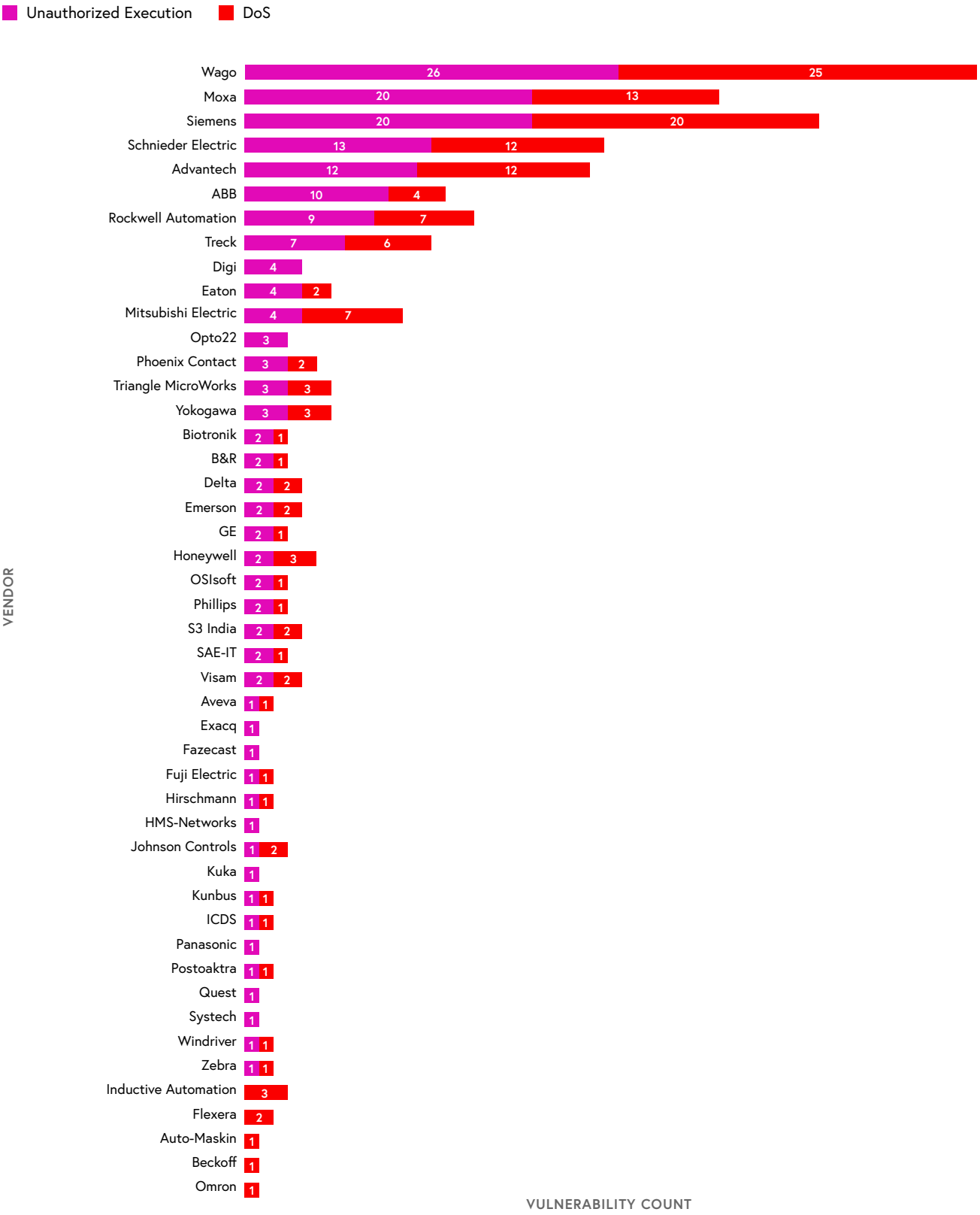


Figure 2.8a: Breakdown by vendor of NVD-published ICS vulnerabilities that can allow for unauthorized code/command execution and/or DoS

A comparison of ICS vulnerability data from 1H 2019 and 1H 2020 shows the longevity of remote code execution, read application data, DoS, and bypass protection mechanisms as the top four most prevalent impacts. The number of vulnerabilities that could result in remote code execution saw a modest decline of 7.7% since last year, while read application (+25.4%), DoS (+9.2%), and bypass protection mechanisms (12.6%) all saw modest but notable increases.

Further down the list of potential impacts, read files or directories increased by 78.0%, modify application data increased by 137.9%, and modify files and directories increased by a whopping 268.8%. Any of these potential impacts on the rise could seriously compromise the integrity and availability of impacted systems, hence the growing efforts of security researchers to identify their presence within ICS devices.

Any of these potential impacts on the rise could seriously compromise the integrity and availability of impacted systems, hence the growing efforts of security researchers to identify their presence within ICS devices.

YEAR-OVER-YEAR COMPARISON OF VULNERABILITY COUNT BY IMPACT

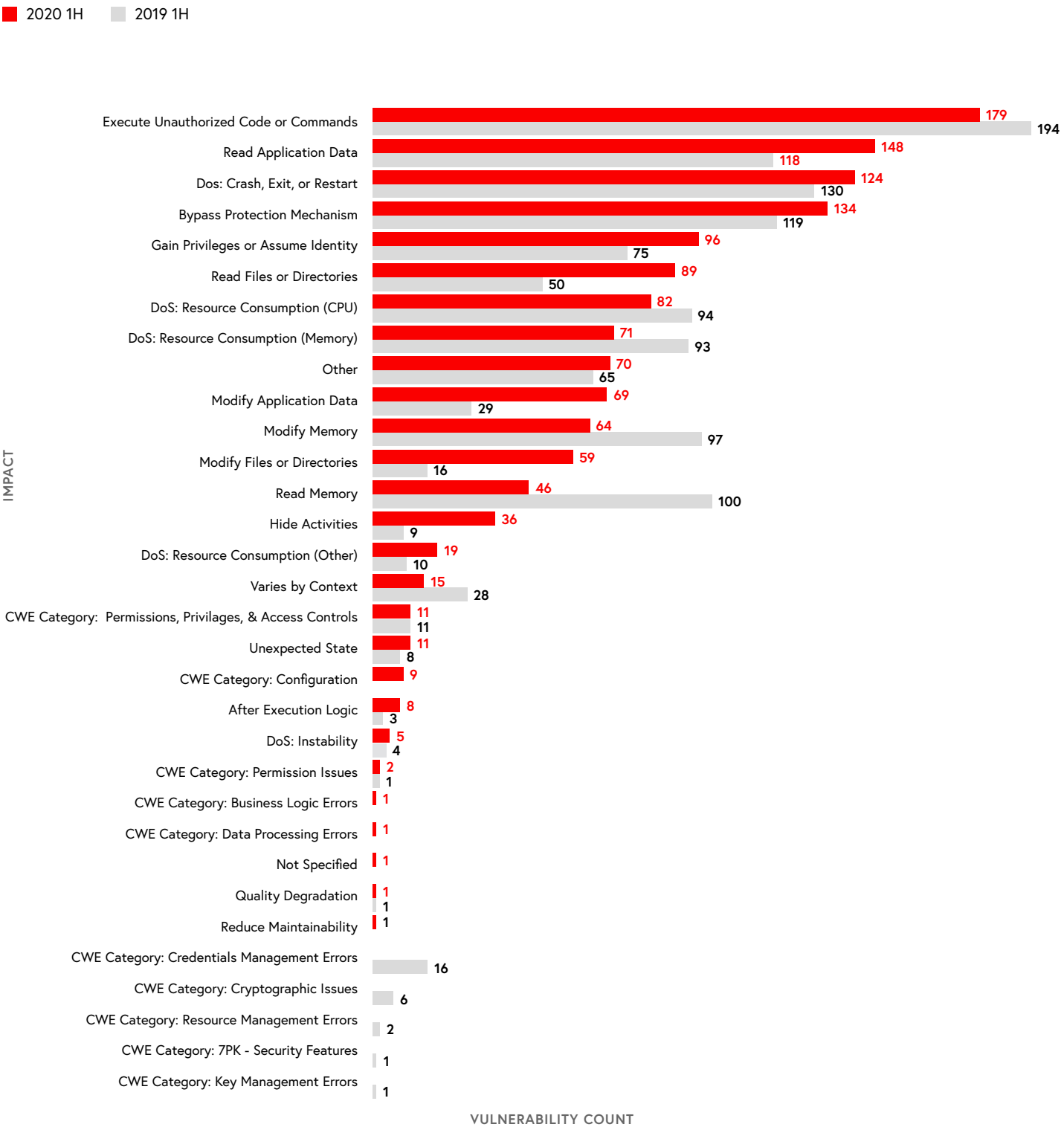


Figure 2.8b: Frequency of potential impacts among ICS vulnerabilities published by the NVD in 1H 2019 vs. 1H 2020

PART 3: KEY EVENTS RELEVANT TO THE 1H 2020 ICS RISK & VULNERABILITY LANDSCAPE

Events ranging from security incidents and regulatory changes to geopolitical developments and global crises, among others, have long helped shape the ICS risk & vulnerability landscape. It is crucial to understand, however, that this relationship is generally one of correlation and influence rather than causation and attribution. Such events are merely one of countless known and unknown factors that define this landscape and its impact on OT security practitioners, the industrial operations they are entrusted to protect, and the ICS community as a whole.

Events ranging from security incidents and regulatory changes to geopolitical developments and global crises, among others, have long helped shape the ICS risk & vulnerability landscape.

That being said, The Claroty Research Team assesses that the following events likely have played a role in shaping the ICS risk & vulnerability landscape to some degree in 1H 2020.

3.1. THE COVID-19 PANDEMIC

As is a fairly common trend during times of crisis, cyber adversaries have been keen to take advantage of the global instability and massive economic, cultural, and behavioral shifts brought on by the COVID-19 pandemic.

Cyber adversaries have been keen to take advantage of the global instability and massive economic, cultural, and behavioral shifts brought on by the COVID-19 pandemic.

Phishing Attacks and Spam Campaigns

The frequency of phishing attacks and spam campaigns began increasing in early 2020 around the same time as COVID-19 was recognized as a global pandemic. In general, this has entailed a proliferation of cyber adversaries registering domains containing terms such as "corona" and "covid19" and creating fraudulent websites from which to spread malware or solicit funds under the guise of pandemic-related health insurance applications or fundraising campaigns.

Cyber Attacks Targeting the Healthcare Sector
Hospitals and medical centers have been targets of ransomware groups for years, but the COVID-19 pandemic appears to have only increased their susceptibility. Adversaries recognize that since these types of institutions are a vital necessity—particularly during times of crisis—they simply cannot afford to lose access to their critical systems and thus tend to be more likely to pay ransoms. Indeed, several targeted ransomware attacks impacted the U.S. and European healthcare sectors during 1H 2020.

Uptick in Remote Workforces
Lockdown and shelter-in-place mandates enacted in light of COVID-19 have required companies globally to find remote alternatives for their employees. In many cases, the rapid increase in remote workers created security gaps and an expanded attack surface for many organizations.

Having quickly realized that targeting remote workers can provide a viable path into enterprise networks—and for industrial enterprises and critical infrastructure organizations, this includes OT networks—adversaries have continued to do so by exploiting unpatched virtual private network (VPN) systems, legacy Windows vulnerabilities, and carrying out phishing attacks, among other methods.

For further information regarding critical infrastructures protection during a crisis, refer to:
https://blog.claroty.com/protecting-critical-infrastructure-is-especially-important-during-a-crisis

3.2. ATTEMPTED CYBER ATTACK ON ISRAELI NATIONAL WATER SUPPLY

In April 2020, an attempted cyber attack targeted the command and control systems of the Israel Water Authority's wastewater treatment plants, pumping stations, and sewage infrastructure. The country's Water Authority and National Cyber Directorate reported that the incident appeared to be coordinated but that no damage had occurred.

This attempted attack highlights that while water infrastructure often eludes the public's attention as a major source of cyber risk, it remains susceptible to both targeted and non-targeted threats. A combination of legacy systems, growing connectivity, and federated management—most water utilities are owned and operated at a local level—warrants a high prioritization of cybersecurity for the water & wastewater sector on a global level.

A combination of legacy systems, growing connectivity, and federated management—warrants a high prioritization of cybersecurity for the water & wastewater sector on a global level.

Reliable and safe access to water plays an essential role in modern life, and now more than ever amid the COVID-19 pandemic, cyber attacks against water infrastructure have high potential to cause a significant threat to public health, making effective vulnerability management an especially high priority for this critical infrastructure sector.

For further information regarding the water supply attack and recommendations, refer to:
https://blog.claroty.com/critical-infrastructure-attack-attempted-against-israeli-water-supply

3.3. DISCLOSURE OF RIPPLE20 VULNERABILITIES

In June 2020, cybersecurity firm JSOF disclosed a set of 19 zero-day vulnerabilities collectively known as Ripple20. The vulnerabilities are present within the Treck TCP/IP stack, which is used by hundreds of millions of devices—including OT and Internet of Things (IoT) devices. For any such devices still in use, the risks are significant and range from DoS activity and data exposure to remote code execution, among others.

The affected vendors range from small shops to major corporations including Schneider Electric, Rockwell Automation, Baxter, Cisco, and more. JSOF identified the industrial, medical, retail, transportation, oil & gas, aviation, and government sectors as particularly affected by the Ripple20 vulnerabilities. The full scope of affected products remains unclear as of this writing.

The Claroty Research Team assisted JSOF by providing consulting services and access to Claroty's extensive ICS lab environment, thereby supporting:

- Identification and validation of devices affected by Ripple20
- Coordination with vendors of the affected devices
- Post-disclosure testing of Ripple20 vulnerabilities on equipment via Claroty's lab

For further information regarding Ripple20, refer to:
https://blog.claroty.com/research/ripple20-new-remote-code-execution-vulnerabilities-affect-millions-of-devices

PART 4: RECOMMENDATIONS

The Claroty Research Team recommends that the following precautionary measures and controls be implemented in order to help minimize the risk and mitigate the impacts of the facets of the 1H 2020 ICS risk & vulnerability landscape described in this report.

4.1. PROTECT REMOTE ACCESS CONNECTIONS

The expansion of remote workforces fueled by efforts to limit the spread of the COVID-19 pandemic continues to have important implications for securing OT networks. Protecting remote access connections is critical. Security practitioners are encouraged to do the following:

- Verify usage of patched VPN versions
- Monitor remote connections, particularly those to OT networks and ICS devices
- Enforce granular user-access permissions and administrative controls
- Enforce multi-factor authentication

4.2. PROTECT AGAINST PHISHING, SPAM, AND RANSOMWARE

The increase in remote work has increased reliance on email as a vital communication mechanism. These conditions thereby also increase the risk of personnel being targeted by phishing or spam attacks and thus ransomware and other malware infections. Security practitioners and all personnel are encouraged to do the following:

- Do not open emails or download software from untrusted sources
- Do not click on links or attachments in emails that come from unknown senders
- Do not supply passwords, personal, or financial information via email to anyone
- Always verify the email sender's email address, name, and domain
- Backup important files frequently and store them separately from the main system
- Protect devices using antivirus, anti-spam and anti-spyware software
- Report phishing emails to the appropriate security or IT staff immediately

4.3. PROTECT INTERNET-FACING ICS DEVICES

If not properly protected, internet-facing ICS devices can provide a pathway into OT networks and the vital industrial processes they underpin. Exacerbating this risk is the fact that adversaries are known to have at their disposal multiple open-source, legitimate, internet-scanning services—such as Shodan.io and Censys.io—to help them identify web-based human machine interfaces (HMIs) and other ICS devices that may have become inadvertently exposed to the internet.

If such a targeted device is password-protected, adversaries have been known to attempt to brute-force their way in. But in many cases, these ICS devices are not password-protected at all, granting adversaries immediate, unfettered access.

At a bare minimum, The Claroty Research Team strongly advises ICS operators to comply with recommendations from Israel's Computer Emergency Response Team (IL-CERT) related to threats targeting critical infrastructure. In addition, OT security teams should also:

- Ensure all internet-connected ICS devices are password-protected and that stringent password hygiene is enforced
- Implement granular role- and policy-based administrative access for all ICS devices and connected systems
- Secure all remote access connections using mechanisms such as encryption, access control lists, and appropriate remote access technologies suitable for OT networks
- Adhere to OT security best practices such as maintaining an accurate asset inventory, properly segmenting OT networks, implementing continuous threat monitoring, and maintaining comprehensive risk and vulnerability management practices

For further information regarding the risks posed by internet-facing ICS devices, refer to:
https://blog.claroty.com/research/internet-facing-ics-devices

ACKNOWLEDGEMENTS

The primary author of this report is Chen Fradkin, Security Research Analyst at Claroty.

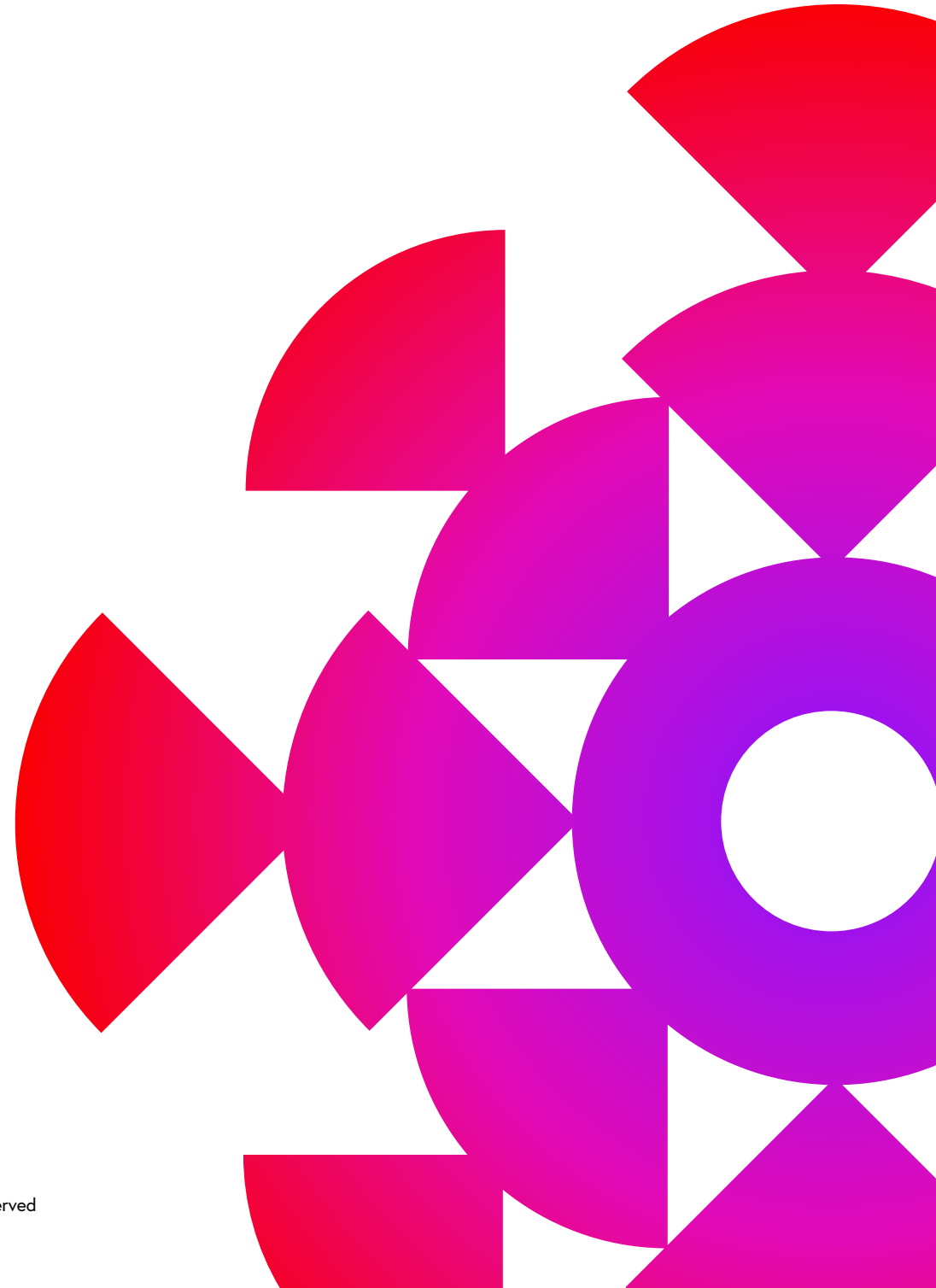
Contributors include Rotem Mesika, Research Analyst Team Lead at Claroty, and Amir Preminger, Vice President of Research at Claroty. Special thanks to the entirety of The Claroty Research Team for providing exceptional support and assistance to various aspects of this report and the extensive research efforts that fueled it.

ABOUT CLAROTY

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with automated production sites and factories that face significant security and financial risks especially need to bridge this gap.

Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.



CLAROTY