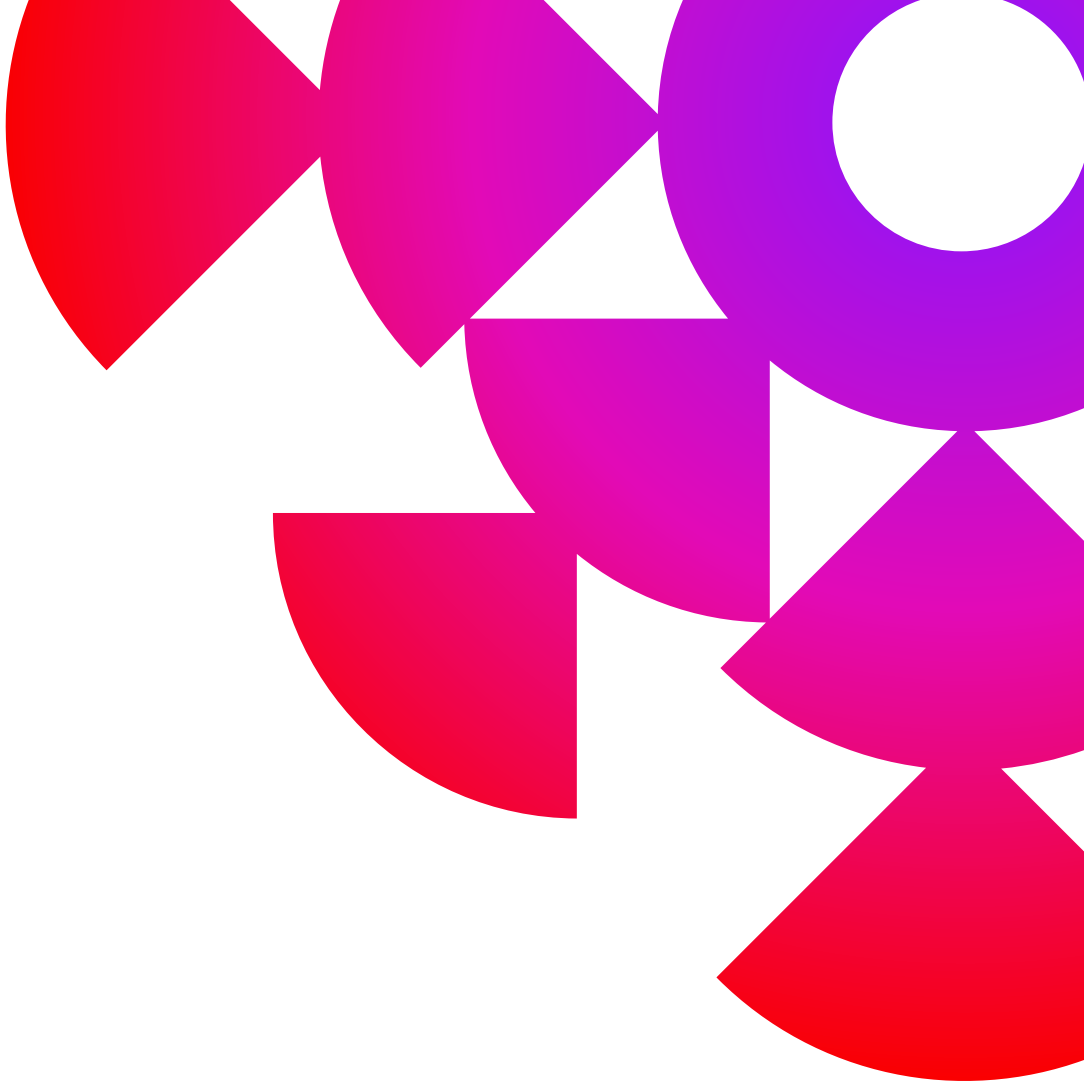


CLAROTY BIANNUAL ICS RISK & VULNERABILITY REPORT: 2H 2020

By the Claroty Research Team

CLAROTY

CONTENTS

EXECUTIVE SUMMARY

Few of us will fondly remember 2020, a transformative year that forced businesses worldwide to rethink and reprioritize remote workforces, their impact on productivity and business continuity, and the expanded attack surfaces consequential to those changes.

Opportunistic attackers went especially low throughout 2020, elevating extortion and ransomware attacks within their arsenals and targeting critical infrastructure and services, such as manufacturing, health care, electric and water utilities, and food and beverage. This dynamic created a race between attackers, researchers, and defenders to find exploitable vulnerabilities, especially in industrial control systems, SCADA control systems, and operational technology (OT) protocols and networks.

These systems and communication protocols oversee industrial processes in dozens of industries, and any weak spot could be a beacon to threat actors keen on accessing the internals of an industrial enterprise and either disrupting or modifying processes central to the business.

Claroty has attempted to define the vulnerability landscape around industrial cybersecurity, and in this, our second Biannual ICS Risk & Vulnerability Report of 2020, our research team presents a comprehensive look at ICS vulnerabilities disclosed publicly during the second half of 2020 (2H 2020). The data presented in this report includes security flaws found by Claroty researchers, as well as those found by independent researchers and experts inside other organizations.

By illuminating current risk and vulnerability trends, we hope to inform OT security managers and operators with additional context around these threats and risks to their environment in order to enhance their decision-making. It is important to note that security incidents that involved ICS vulnerabilities disclosed in 2H 2020 are not a focal point of this report because such incidents—whether ICS-targeted or opportunistic attacks—can skew the perceptions of the prevalence and impact of a given vulnerability.

Key data points in this report include:

ICS SECURITY RESEARCH AND DISCLOSURE TRENDS

- During 2H 2020, 449 vulnerabilities were disclosed affecting ICS products from 59 vendors. More than 70% of those flaws were assigned high or critical Common Vulnerability Scoring System (CVSS) scores, down from more than 75% in 1H 2020.
- The number of ICS vulnerabilities disclosed in 2020 increased by 32.89% compared to 2018 and 24.72% compared to 2019. The primary factors for the increase 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.

- Vulnerabilities in ICS products disclosed during 2H 2020 are most prevalent in the critical manufacturing, energy, water and wastewater, and commercial facilities sectors—all of which are designated as critical infrastructure sectors.
- The number of vulnerabilities affecting the commercial facilities sector increased by 140% compared to 2H 2018.
- The number of vulnerabilities affecting the government facilities sector increased by 780% compared to 2H 2018.
- 60.8% of vulnerabilities were discovered by third-party companies making them the most dominant research group. Among all third-party companies, there were 22 that reported their first disclosures, further evidence of growth in the ICS vulnerability research market.

THREATS AND RISKS FROM ICS VULNERABILITIES

- 71.49% of the vulnerabilities are exploited through a network attack vector (i.e. remotely exploitable).
- 46.32% of vulnerabilities found affect the Basic Control (Level 1) and Supervisory Control (Level 2) levels of the Purdue Model.
- 14.7% of vulnerabilities found affect multiple types of products (operating at various OT Purdue Model levels, IoT, and network devices). This category mostly contains vulnerabilities in third-party components.
- 89.98% of vulnerabilities don't require special conditions to exploit, and an attacker can expect repeatable success every time.
- In 76.39% of the vulnerabilities, the attacker is unauthenticated prior to attack and doesn't require any access or privileges to the target's settings or files.
- For 78.17% of the vulnerabilities, there is no requirement for user interaction.
- 78.92% of the vulnerabilities that don't require user interaction are remotely exploitable.
- For 80.95% of the Supervisory Control vulnerabilities, user interaction is needed if exploiting via a local attack vector. This indicates a playground for social engineering attack vectors.
- If exploited successfully, 65.7% of the vulnerabilities can cause total loss of availability.
- For 94.43% of the vulnerabilities, the impact to confidentiality is low or none, and for 80.4% of vulnerabilities the impact to integrity is zero. This demonstrates that while integrity and confidentiality of information is important in IT security, it is a lesser risk variable in OT networks, requiring further severity assessment of each vulnerability.
- The top five most prevalent Common Weakness Enumerations (CWEs), manifested in the ICS vulnerabilities disclosed during 2H 2020 are all ranked highly on The MITRE Corporation's 2020 CWE Top 25 Most Dangerous Software Weaknesses list, due their relative ease of exploitation and high potential impacts.

THINGS TO CONSIDER

Now that we've shared some data from our analysis of the ICS vulnerability landscape, it's important to discuss what's happening behind the numbers and not only address why we're seeing steady growth in the number of security flaws discovered, reported, fixed, but also why they're confined to a relatively small number of prominent vendors.

For context, it's important to remember that industrial control systems and other field devices have extensive shelf lives. Unlike IT software, applications, and hardware appliances that have regular update and buying-turnover cycles, ICS gear and operational technology are designed to last considerably longer. Much of this equipment runs critical infrastructure and manufacturing processes in industries that are pivotal to the global economy. Taking down an industrial control system or specific process-oriented device for a firmware or software update is no simple feat in industries where uptime, reliability, and safety are paramount.

DIGITAL TRANSFORMATION

Some of the increased focus on ICS vulnerabilities from security companies and independent researchers—not to mention threat actors—mirrors the convergence of IT and OT networks. These synergies will enhance the efficiency of industrial processes and save money across the board, but they also can increase the attack surface available to adversaries. Some attacks that originate on IT networks via well-known vectors—such as phishing, malware, or exploits of known flaws—may cross over to industrial networks. Engineering workstations, for example, traverse both networks and can be a linchpin that allows denial-of-service or ransomware attacks to affect both IT systems and ICS devices, thus impacting industrial processes.

As the leading industrial cybersecurity company, Claroty has a unique perspective on the ICS vulnerability landscape. The Claroty Research Team makes it a priority to examine the vulnerable attack surface areas most impacted by digital transformation initiatives and share our extensive vulnerability reports and analysis with the community at large.

The Claroty Research Team works through the Purdue Model for ICS security, focusing on gaining remote access to the corporate network in order to move through the IT/OT DMZ to reach process and control networks, as well as field devices. In the second half of 2020, we once again saw a significant number of remotely exploitable vulnerabilities reported to vendors and disclosed by organizations such as ICS-CERT, CERT@VDE, and MITRE. We need to stress the importance for defenders to focus on comprehensive remote access solutions that are ICS and OT-specific and understand the communication protocols at play here. Network segmentation and network-based detection are fundamental to defense-in-depth and are also mandates to protect converged IT/OT networks.

MATURATION OF ICS SECURITY RESEARCH

We also saw a high concentration of disclosed vulnerabilities centered around leading industrial vendors, such as Schneider Electric, Mitsubishi, and Siemens. These automation vendors, along with Rockwell Automation, GE, and others, are the backbone of industrial enterprises. Researchers—and threat actors—concentrate on the highest-value targets. Since these vendors own a good amount of market share and have deep penetration into businesses in critical industries, they present the most likely targets of opportunity, therefore receiving the most scrutiny from white hats and black hats alike.

If all of this sounds familiar, you're right. It's not too dissimilar from the early days of the maturation of IT security, when Microsoft was under constant pressure from customers and security companies to lock down its products and install a secure development lifecycle. Microsoft Windows was the desktop operating system leader then, and now, with more than 75% of market share. With that came relentless attacks from threat actors and discovery after discovery of vulnerabilities by researchers, resulting ultimately in the Trustworthy Computing initiative and regular patch cycles. Other tech giants, such as Oracle and Apple, soon followed that model and instituted their own regular cycle for security updates.

The steady growth of reported ICS vulnerabilities is noteworthy in terms of maturation, but currently, it's also largely limited to three vendors: Schneider, Mitsubishi, and Siemens. A large majority of the products with disclosed and patched vulnerabilities in the 2H of 2020 belong to those three leading vendors; the remaining vendors had combined relatively fewer products affected by vulnerabilities.

Does this mean that the smaller number of vendors we looked at have cleaner, more secure products? Likely, no. Instead, it's more of an issue of accessibility to equipment for a growing number of researchers; market leaders have an abundance of equipment inside organizations that can be assessed for security flaws. Some of this gear that has been retired can also be purchased on eBay and other platforms for research purposes.

ADVERSARIES

As for adversaries, while there wasn't a Triton-scale attack in 2020, threats continue to surface from nation-state actors (cyberattacks against the Israel Water Authority, and the SolarWinds supply-chain attack) and cybercriminals (the inclusion of ICS processes in the SNAKE ransomware kill list). As we mentioned earlier, breaching the corporate perimeter is the first hop on the Purdue Model, and while network defenses may be enhanced, incidents such as the SolarWinds attack demonstrate the fragility of some perimeter-based defenses and the eventuality that these attacks will land on ICS and SCADA equipment.

Compounding the risk is the fact that attacks against ICS devices and OT networks tend to be targeted. While ICS and SCADA vulnerability research is maturing, there are still many decades-old security issues yet uncovered. For the time being, attackers may have an edge in exploiting them, because defenders are often hamstrung by uptime requirements and an increasing need for detection capabilities against exploitable flaws that could lead to process interruption or manipulation.

ABOUT THE CLAROTY RESEARCH TEAM

The Claroty Research Team is an award-winning group of OT researchers, known 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.

To date, The Claroty Research Team has discovered and disclosed more than 70 ICS vulnerabilities, 41 of which were disclosed during the 2H of 2020.

Recognizing the critical need to understand the ICS risk and vulnerability landscape and how the vulnerabilities discovered by Claroty researchers fit into that picture, The Claroty Research Team developed an automated collection and analysis tool that ingests ICS vulnerability data from trusted open sources, including the National Vulnerability Database (NVD), the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), CERT@VDE, MITRE, and industrial automation vendors Schneider Electric and Siemens.

The outputs of this tool exposed key trends and contextualized implications pertaining to ICS vulnerabilities, the risks they pose to industrial 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 2H 2020

Claroty researchers discovered and disclosed 41 vulnerabilities during the 2H 2020 and represent the direction and core objectives of the team's research focus. Overall, Claroty researchers have found and disclosed more than 70 ICS vulnerabilities.

The Claroty Research Team prioritizes its research on industrial control systems on a number of parameters to provide the greatest benefit and contribution to the ICS domain and security community by examining industrial devices, protocols, and networks. Claroty is in tight communication with vendors and partners and receives input and requests regarding specific products and versions. Some of the team's research parameters include:

- Commonality of the platform, device or equipment
- Potential damage from an attacker discovering and exploiting a vulnerability in the product before the vendor patches it
- How many devices will be affected by the vulnerability
- Products that are in use by Claroty customers

Claroty's research examines a variety of vendors and products affecting numerous sectors in the industry. Because of these exact parameters, Claroty also researches third-party products, and among the vulnerabilities disclosed by Claroty during 2H 2020, 14 were third-party.

1.1. AFFECTED ICS VENDORS

Many of these vendors have products widely deployed across critical industrial markets globally, a key factor in the Claroty Research Team's decision to focus on them.

A breakdown of the 14 vendors affected by the 41 vulnerabilities discovered and disclosed by Claroty in 2H 2020 is as follows.

VENDORS

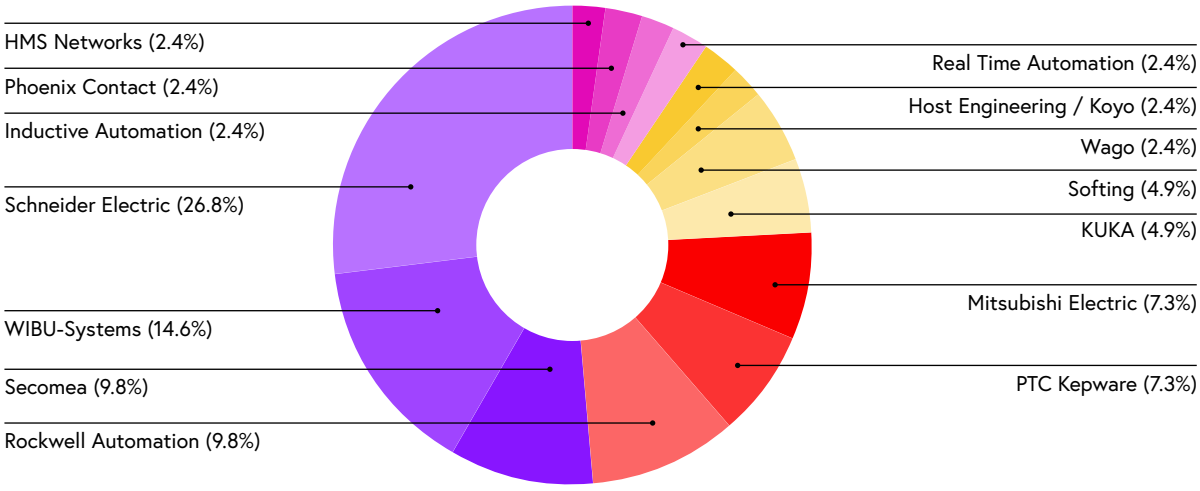


Figure 1.1: Breakdown of Claroty-discovered vulnerabilities by affected vendors

1.2. AFFECTED ICS PRODUCT TYPES

In the following graph, you can see the distribution of the targeted products Claroty researched.

Of note, Claroty discovered and disclosed 10 vulnerabilities affecting products at Level 2 of the Purdue Model for ICS security, the process network. This level includes SCADA servers, Human Machine Interfaces (HMIs), and other equipment overseeing industrial processes.

Claroty researchers also found eight vulnerabilities at Level 1, the control network, which is home to programmable logic controllers (PLCs) and remote terminal units (RTUs). Both of these systems monitor and control field devices, such as pumps, valves, fans, and actuators. Eight vulnerabilities were also identified and disclosed affecting products at Level 3, the operations level of the Purdue Model. These would include control system historians that gather and store data from devices, as well as domain controllers, database servers, engineering workstations, and other critical operational systems.

TARGETED PRODUCT FAMILY

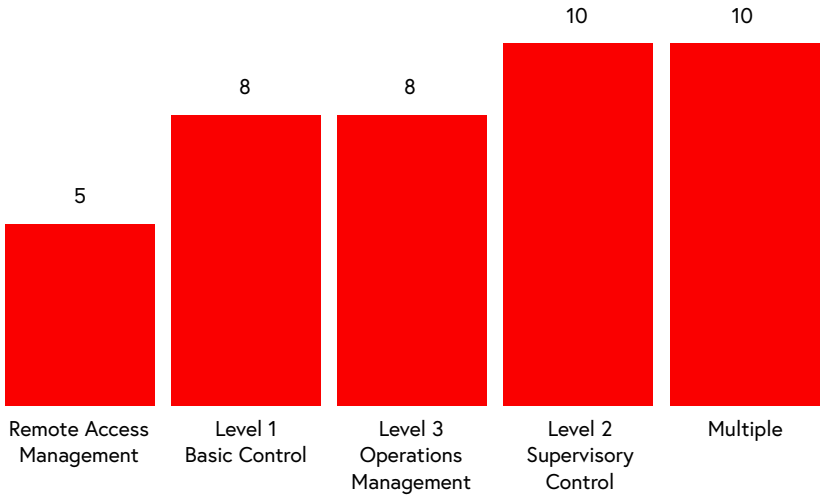


Figure 1.2: Breakdown of Claroty-discovered vulnerabilities by product type according to the Purdue Model.

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

This section provides a statistical analysis and contextual assessment of all the ICS vulnerabilities published in 2H 2020.

These include the 41 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. Claroty's sources of information include the National Vulnerability Database (NVD), ICS-CERT, CERT@VDE, Siemens, Schneider Electric, and MITRE.

2.1. TOTAL COUNT OF ICS VULNERABILITIES

VULNERABILITIES PUBLISHED

449

Total ICS Vulnerabilities Published in 2H 2020

VENDORS AFFECTED

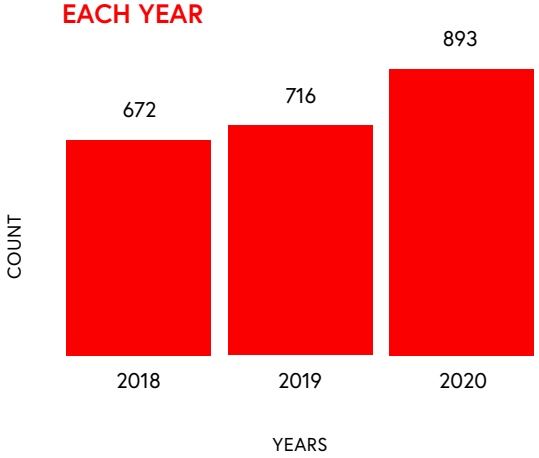
59

Total Vendors Affected by ICS Vulnerabilities

YEAR-OVER-YEAR COMPARISON OF ICS VULNERABILITIES

A breakdown of ICS vulnerability disclosures spanning the last three years shows consistent growth since 2018 indicating an increase of awareness and in the number of security researchers looking at ICS and SCADA equipment for security flaws.

VULNERABILITIES DISCOLOSED EACH YEAR



2.2 ORIGIN OF VULNERABILITY DISCOVERIES, 2H 2020

More than ever, third parties are finding security vulnerabilities in ICS products, rather than the proper vendor behind the product.

In 2H 2020, 84.63% of vulnerabilities disclosed were discovered by external sources. The external sources include a number of research organizations, including third-party companies, independent researchers, and academics, among others.

VULNERABILITY RESEARCH ORIGIN

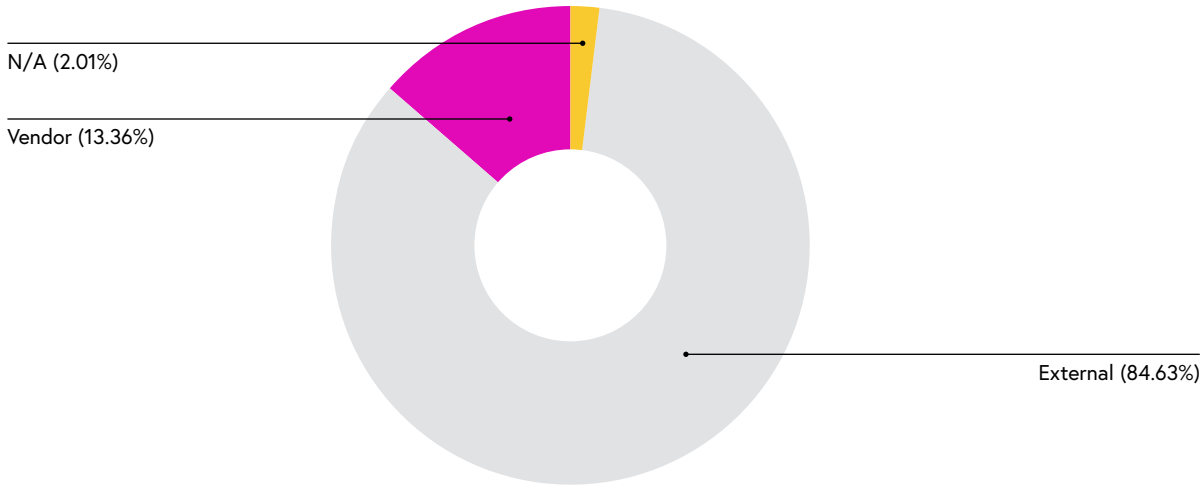


Figure 2.2a: Breakdown of vulnerabilities by origin of discovery

The chart below breaks down the number of vulnerabilities disclosed by external sources, led by third-party companies, which found 273 vulnerabilities in 2H 2020, or 60.8%. Many of these disclosed vulnerabilities were discovered by researchers at cybersecurity companies, indicating a shift in focus to include industrial control systems alongside IT security research. It is important to mention that some disclosures are a collaboration between multiple research groups, or in other cases, different researchers who discovered and disclosed the same vulnerability separately (in 2H 2020, this accounts for 70 vulnerabilities).

RESEARCH GROUP

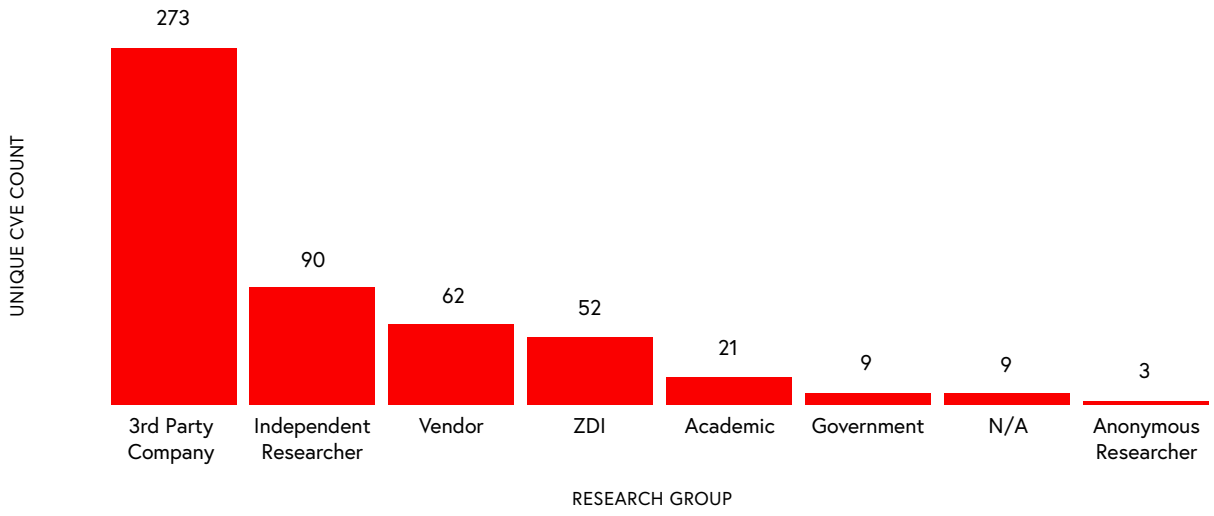


Figure 2.2b: Breakdown of vulnerability discovery by research group.

It is interesting to note that the number of disclosures coming from the Zero Day Initiative (ZDI), a third-party vulnerability company that works with researchers and offers rewards for zero-day vulnerability reports, has dropped since 2018. In 2020, ZDI hosted the first Pwn2Own contest, with an exclusive focus on ICS and SCADA vulnerabilities.

- 2020: ZDI was credited with 11.08% of vulnerabilities.
- 2019: ZDI was credited with 12% of vulnerabilities.
- 2018: ZDI was credited with 16.81% of vulnerabilities.

There are two likely reasons for this phenomenon:

- The increase in the ICS research vulnerability market. The data showed that over the past three years, some names that started as independent researchers who participated in bounty programs such as ZDI have now joined private companies. Claroty also noted a decrease in independent researchers' share of disclosures compared to 2018 (16.79% in 2020 vs. 25.29% in 2018)
- In many cases, independent researchers post in their GitHub repository or private blog and contact the vendors for disclosure through different coordinators—not necessarily ZDI.

The data in the chart below illustrates new entrants into ICS vulnerability research.

Claroty found 50 new researchers who published vulnerability disclosures in 2H 2020 who had not published in 2018 or 2019.

NEW RESEARCHERS PER GROUP TYPE

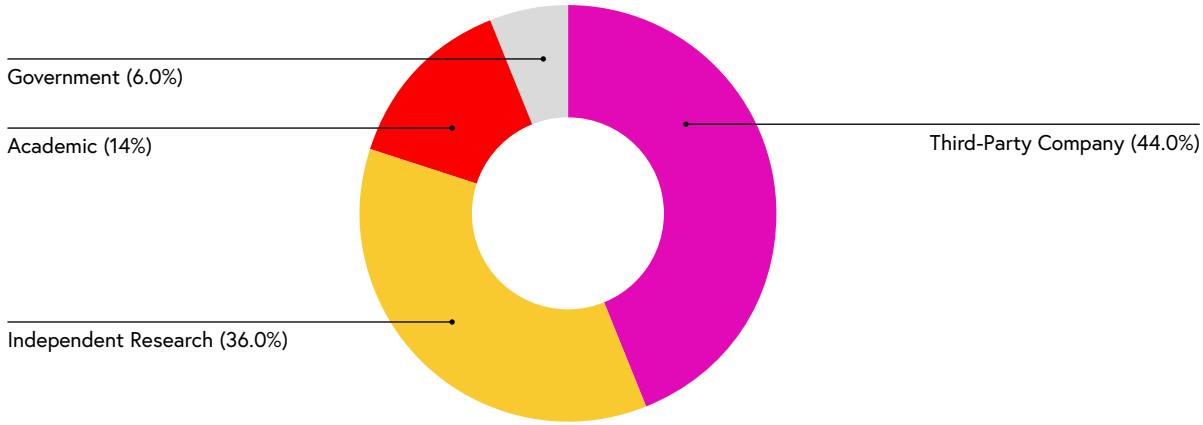


Figure 2.2c: Breakdown of new researchers reporting ICS vulnerabilities.

Claroty's data also indicates that new researchers focused on market-leading vendors, such as Schneider Electric, Siemens, and others. Only five of the 50 new researchers introduced four newly affected vendors in 2H 2020. The remainder examined previously affected vendors, including 13 new researchers reporting bugs in Schneider Electric products, and nine new researchers reporting bugs in Siemens products.

2.3 AFFECTED ICS VENDORS

The 449 ICS vulnerabilities disclosed in 2H 2020 affected products from 59 vendors. ICS automation vendor Schneider Electric led the pack, with 80 vulnerabilities affecting its products, trailed closely by Siemens, Mitsubishi, Philips, and Advantech.

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.

VULNERABILITIES PER VENDOR

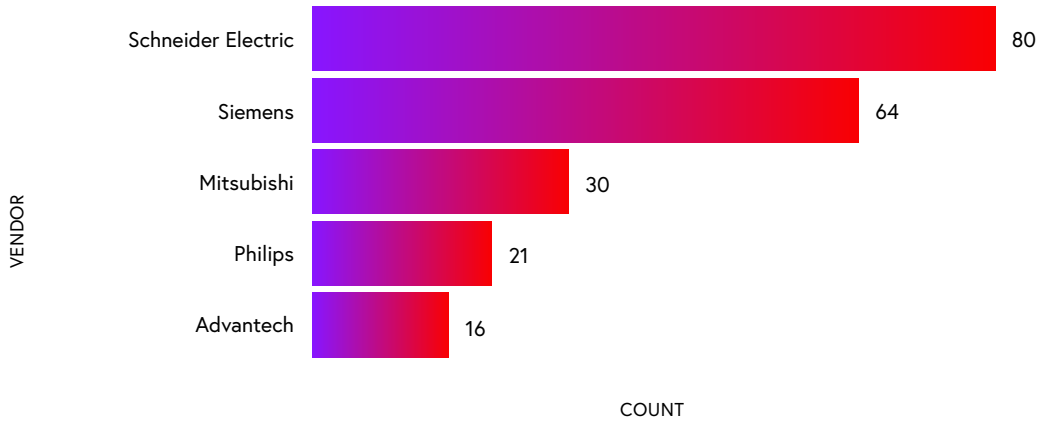


Figure 2.3a: Breakdown of ICS vulnerabilities by the most affected vendors.

ICS VENDORS NEWLY AFFECTED BY VULNERABILITIES IN 2H 2020

During 2H 2020, 14 vendors whose products had not been affected by any ICS vulnerabilities disclosed in 2019 and 1H 2020 were affected by at least one ICS vulnerability disclosed in 2H 2020.

- Four of these vendors specialize in manufacturing, and two specialize in automation, transportation, or medical technologies.
- Vulnerabilities affecting these newly affected vendors (10 of the 14) were uncovered by researchers who had previously disclosed flaws.

Vendors	Primary Industry
Secomea	Remote Access Solution
SHUN HU Technology Co. Ltd	Communications
B. Braun	Medical
OpenClinic GA - open-source collaboration on Source Forge	Medical
Grundfos	Manufacturing, Mechanical Engineering
Host Engineering	Manufacturing
National Instruments Corp. (NI)	Automation, Measurement
NEXCOM	Multiple
Bender	Information Technology, Manufacturing
ARC Informatique	ICS Software
MB connect line	Networking
Multiple Trailer and Brake Manufacturers	Transportation, Manufacturing
PTC	Information Technology
FATEK Automation	Automation, Transportation, Energy

AFFECTED ICS PRODUCTS

FIRMWARE/SOFTWARE

For each disclosed vulnerability, we tagged the vulnerable component as firmware or software. There are cases in which a vulnerability affects several components that are a mix of both. The division seems tight, but given the comparative ease in patching software over firmware, defenders have the ability to prioritize patching within their environments.

FIRMWARE/SOFTWARE

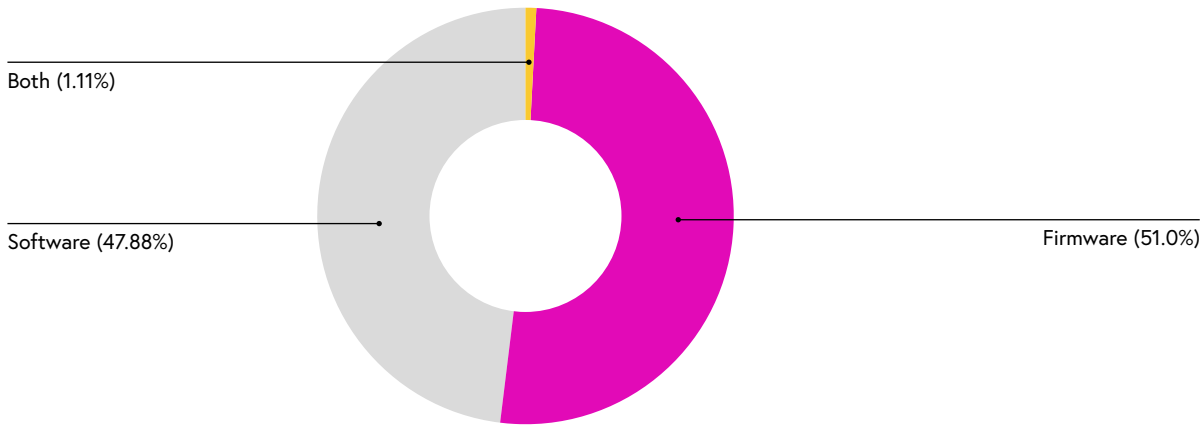


Figure 2.3b: Breakdown of vulnerabilities in software and firmware.

PRODUCT FAMILY CATEGORIES

There is a more interesting division when examining firmware and software vulnerabilities within product families.

It is important to understand that while a vulnerability is found within a component that can be categorized into firmware or software, we need to take into consideration the products affected by it.

For example, there could be a vulnerable software configuration running on HMIs, or maybe an ethernet module connected to a pump. The following graph showcases the "families" of products affected by these vulnerabilities, and the categories are:

- Level 0: Process: Sensors, I/O, etc.
- Level 1: Basic Control: PLC, RTU, controller, etc.
- Level 2: Supervisory Control: HMI, SCADA, Engineering Workstation, etc.
- Level 3: Operations Management: Historian, OPC Server, etc.
- Network Device: Switch, router, gateway, etc.
- IoT: IP cameras, Smart home devices, etc.
- Medical devices and software: Imaging and ultrasound, patient monitors, etc.
- Multiple: When the vulnerability affects numerous categories

AFFECTED PRODUCT FAMILIES

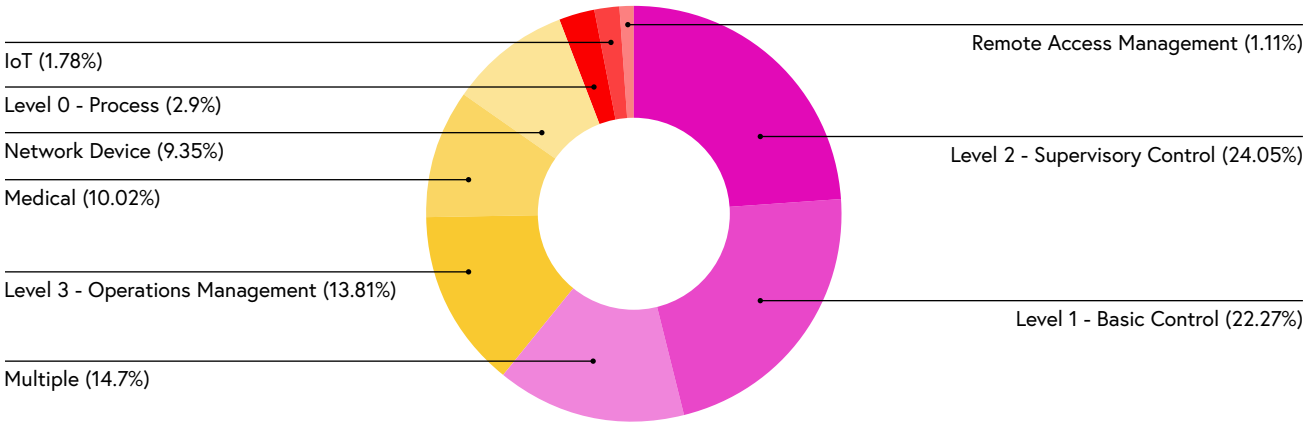


Figure 2.3c: Breakdown of affected product families.

46.32% of vulnerabilities found affect the Basic Control (Level 1) and Supervisory Control (Level 2) levels of the Purdue Model. Naturally, when affecting these levels, an attacker can also reach lower levels and affect the process itself which makes them an attractive target.

In third place, you can see the Multiple category—this category mostly contains third-party vulnerabilities (we had many of these during the past year), which often come in "bundles" of multiple vulnerabilities in each research and disclosure process. They often affect many vendors and products across the industry; one example would be AMNESIA:33. It emphasizes that employing protection and mitigation against third-party vulnerabilities, starting with visibility and risk assessment and management, are an integral part of security in OT networks.

When looking into each category, you can divide the vulnerable component affecting them into firmware, software, or both. Most of the Supervisory Control (Level 2) vulnerabilities are software based, compared to Basic Control (Level 1) vulnerabilities, where the majority are firmware based. With the inability to patch over time, especially in Level 1 device firmware, it is recommended to invest in segmentation, remote access protection, and protection of the Supervisory Control level as it leads to the Basic Control level.

FIRMWARE/SOFTWARE DIVISION IN PRODUCT FAMILY

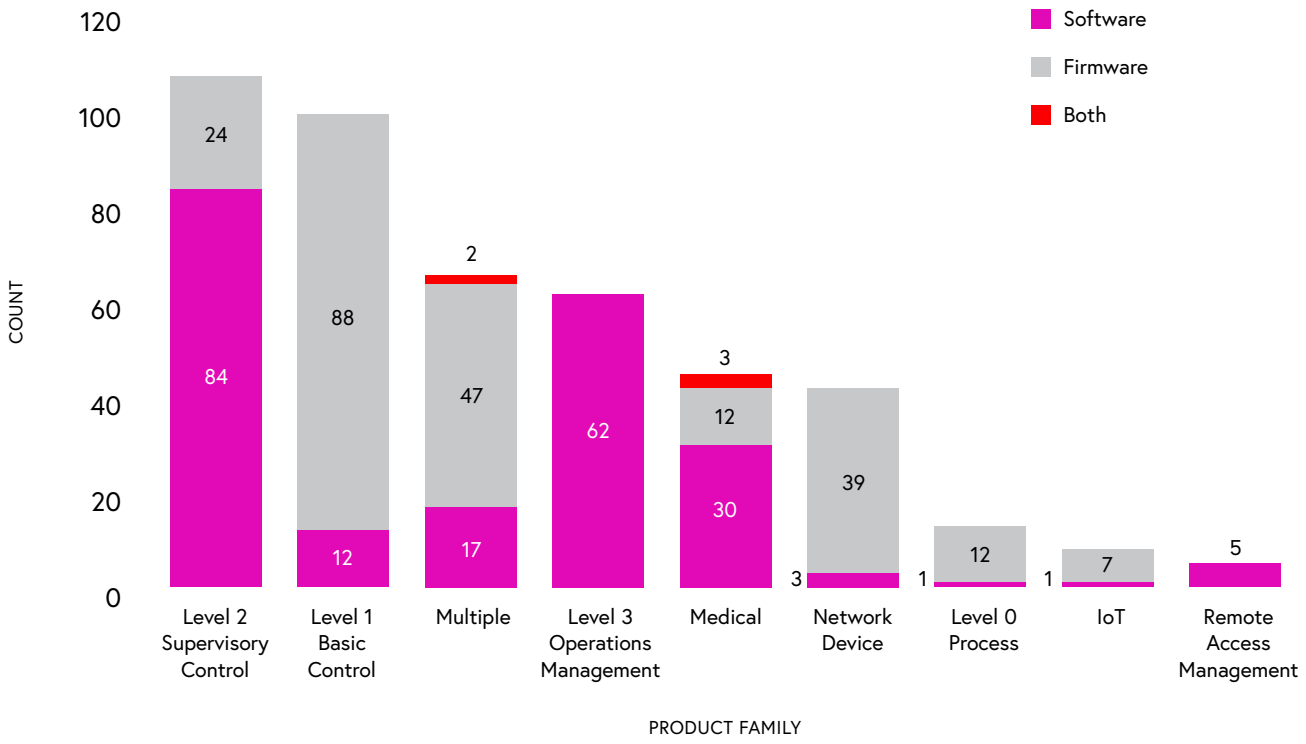


Figure 2.3d: Breakdown of firmware and software vulnerabilities by product families.

2.4 IMPACT OF ICS VULNERABILITIES BY INFRASTRUCTURE SECTOR

The critical manufacturing, energy, water and wastewater, and commercial facilities sectors, all of which are designated as critical infrastructure sectors, were by far the most impacted by vulnerabilities disclosed during 2H 2020.

The commercial facilities sector experienced a 13.68% and 140% increase in vulnerabilities, compared to 2H 2019 and 2H 2018 respectively, while the critical manufacturing (15.48% and 65.81%) and energy sectors (7.51% and 73.83%) experienced similar increases. The government facilities sector increased by 131.58% and 780%, compared to 2H 2019 and 2H 2018. There was a single vulnerability disclosure in 2H 2020 affecting the nuclear reactors, materials, and waste sector, which was not affected by any vulnerabilities disclosed during either 2H 2018 and 2H 2019.

VULNERABILITY COUNT BY INFRASTRUCTURE SECTOR

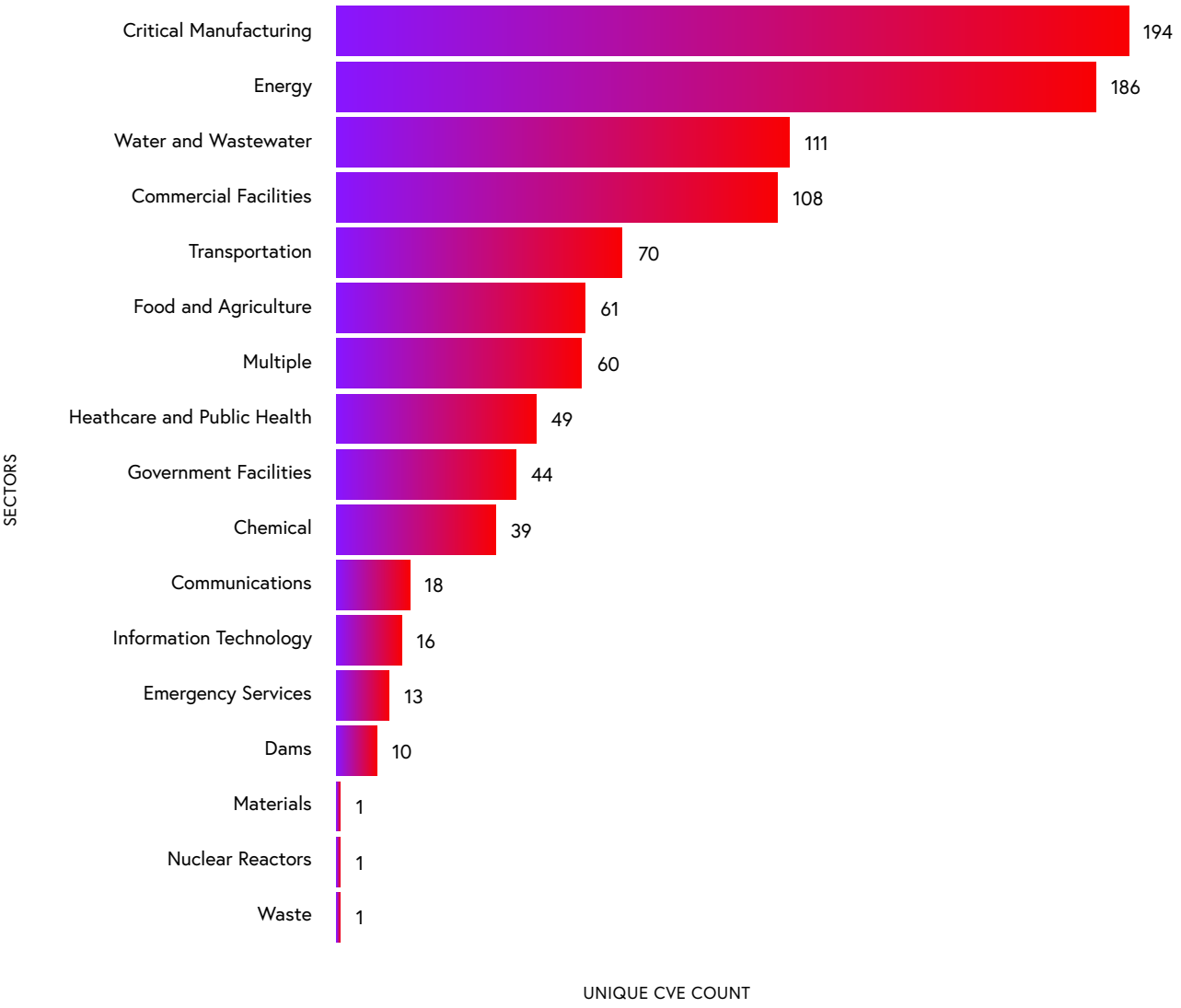


Figure 2.4a: Breakdown of vulnerability counts by infrastructure sector for 2H 2020.

Year-over-year, the chart below shows continuing growth in vulnerabilities disclosed in critical infrastructure sectors, almost uniformly across the board in all but a few sectors.

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

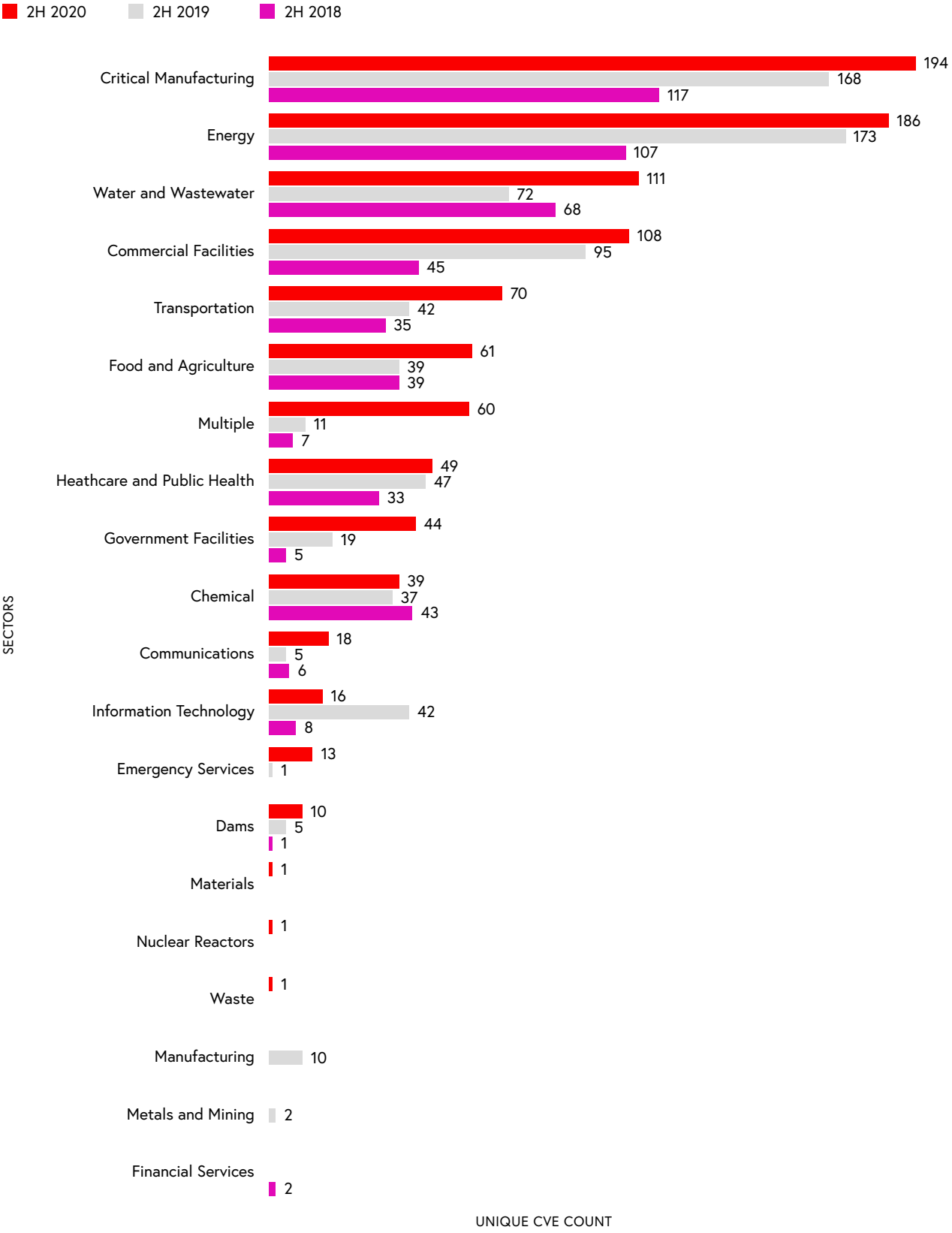


Figure 2.4b: Breakdown of vulnerabilities in critical infrastructure sectors year-over-year.

A monthly breakdown of vulnerabilities indicates that the critical manufacturing, energy, water and wastewater, and commercial facilities sectors were affected by multiple vulnerabilities disclosed during every month of 2H 2020.

MONTHLY COMPARISON OF VULNERABILITY COUNT BY INFRASTRUCTURE SECTOR

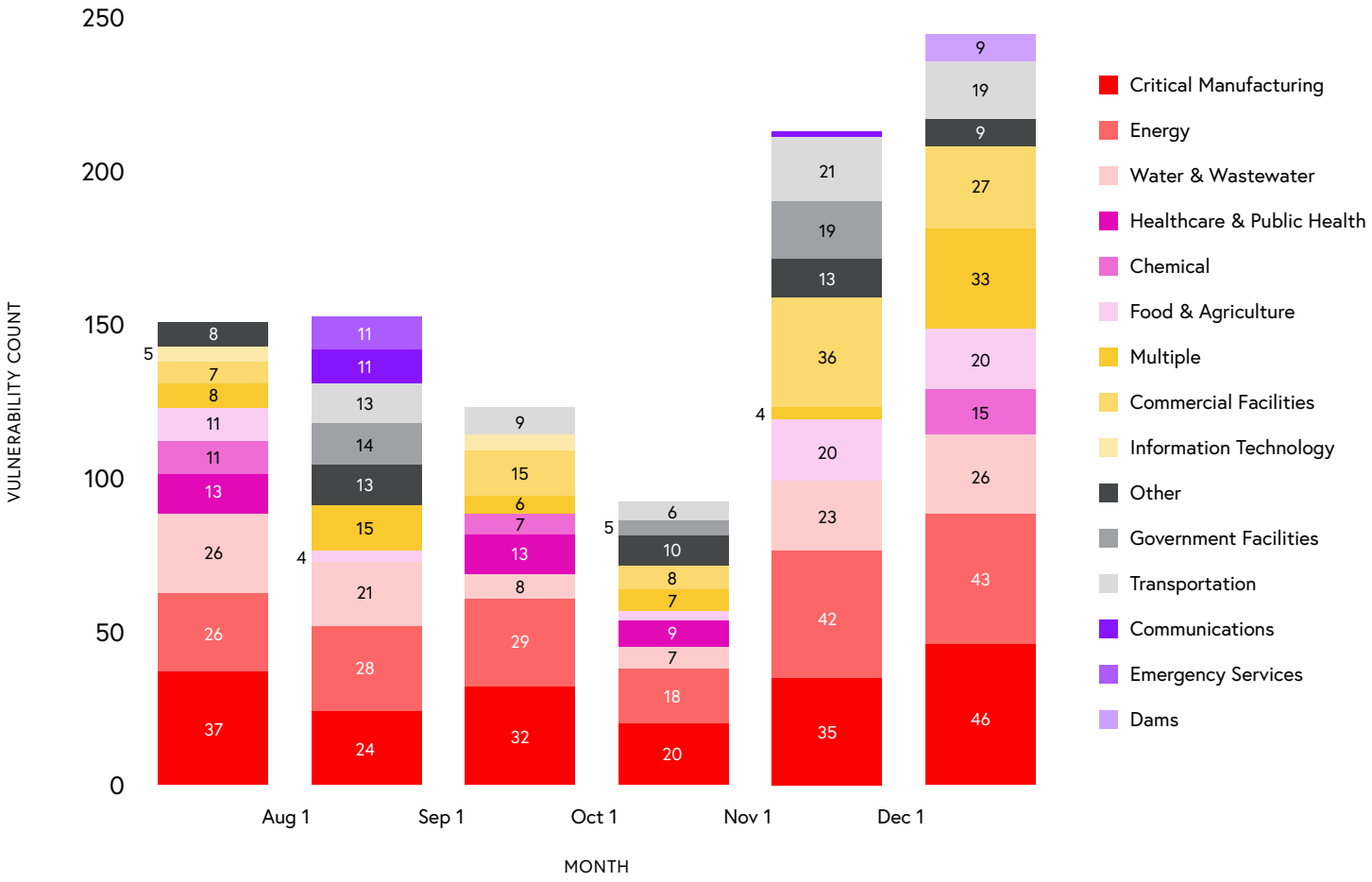


Figure 2.4c: 2H 2020 monthly breakdown of vulnerabilities by infrastructure sector.

PART 3: CVSS INFORMATION

3.1 BASE METRICS

The Common Vulnerability Scoring System (CVSS) is composed of three metrics groups: the first one being the "Base Metrics" group, which represents the characteristics of a vulnerability that are constant over time and user environments and includes two sets of metrics: Exploitability and Impact.

EXPLOITABILITY METRICS

These metrics represent the technical means and difficulty by which vulnerabilities can be exploited.

ATTACK VECTOR

As you can see in the following graph, 71.49% of the vulnerabilities are exploited through a network attack vector and are remotely exploitable. This emphasizes the importance of protecting remote access connections and internet-facing ICS devices.

As for vulnerabilities with a local attack vector: in 54.12% of them, the attacker relies on user interaction to perform actions required to exploit these vulnerabilities. This would include social engineering techniques such as phishing and spam. Awareness and protection against them is critical.

ATTACK VECTOR DISTRIBUTION

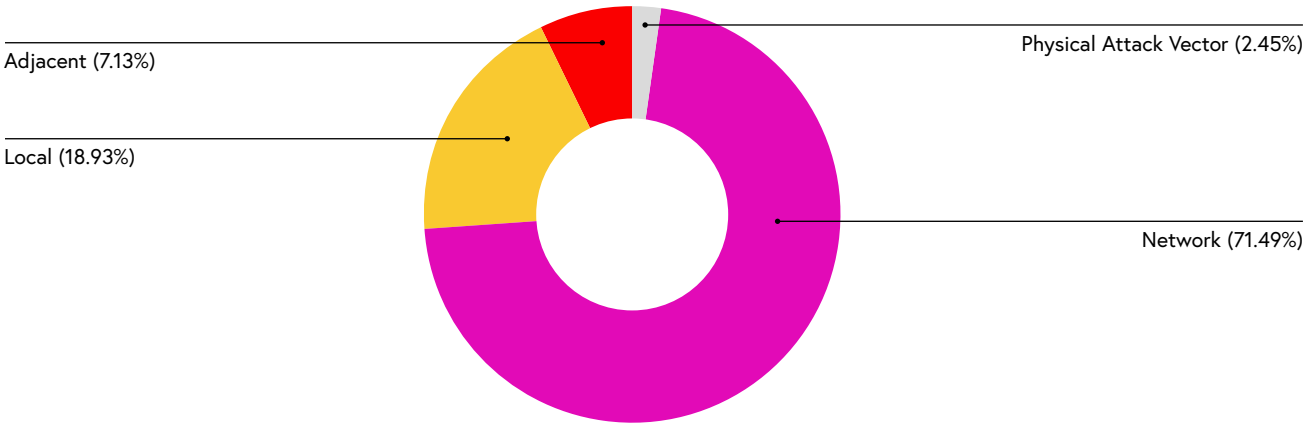


Figure 3.1a: Breakdown of attack vectors associated with ICS vulnerabilities.

The local attack vector is mostly dominant in the Supervisory Control level. Moreover, in 80.95% of the Supervisory Control vulnerabilities via a local attack vector, user interaction is required for exploitation.

The attackers' dependence on user interaction shows the importance of awareness and protection against social engineering tactics among workers with access to critical assets, such as HMIs, SCADA, and engineering stations.

ATTACK VECTOR PER PRODUCT FAMILY

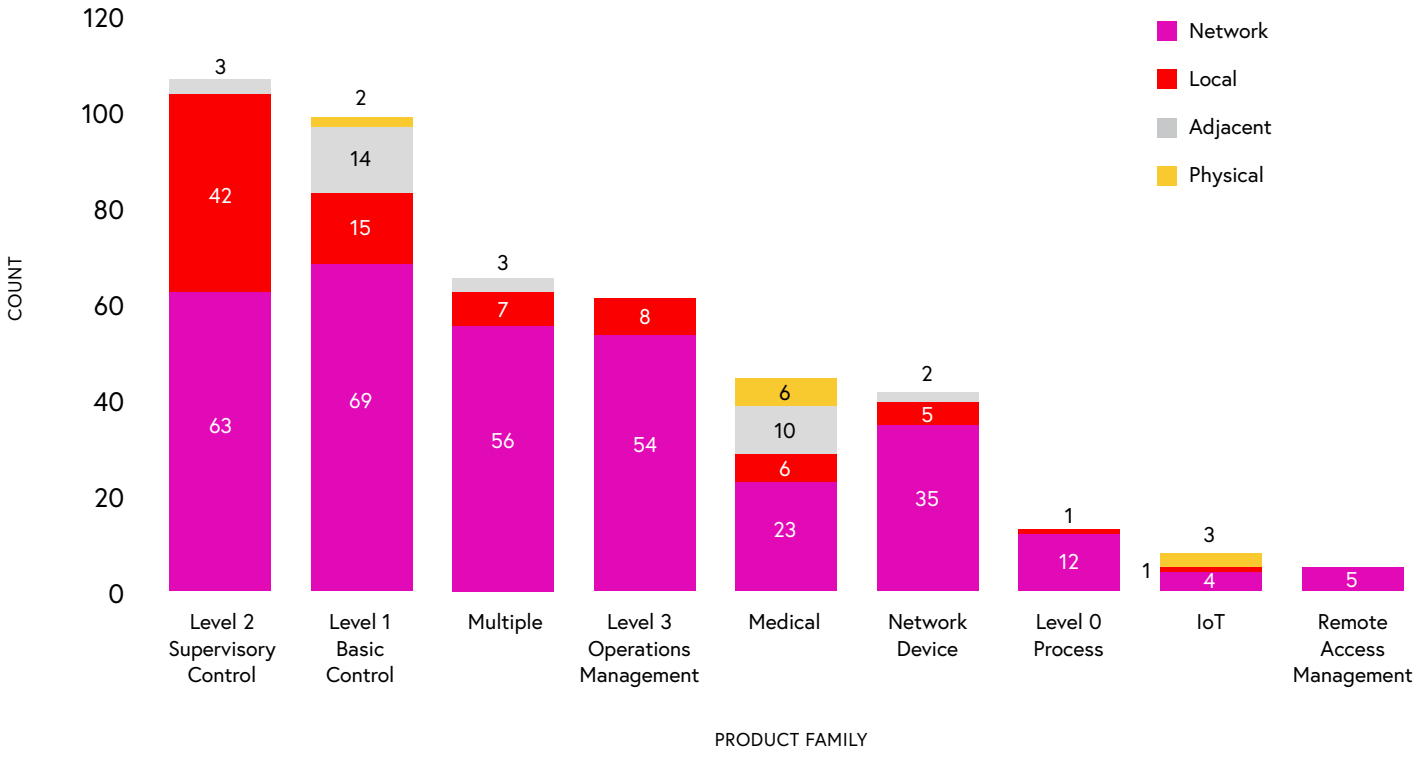


Figure 3.1b: Breakdown of attack vectors by product family.

ATTACK COMPLEXITY

This metric represents the conditions beyond the attacker's control that must exist in order for them to be able to exploit the vulnerability. For example, a successful attack could depend on an attacker gathering knowledge of configuration settings.

For 89.98% of the vulnerabilities, the complexity of exploitation and attack is considered low, meaning that more than 89.98% of vulnerabilities don't require special conditions and an attacker can expect repeatable success every time.

CVSS ATTACK COMPLEXITY

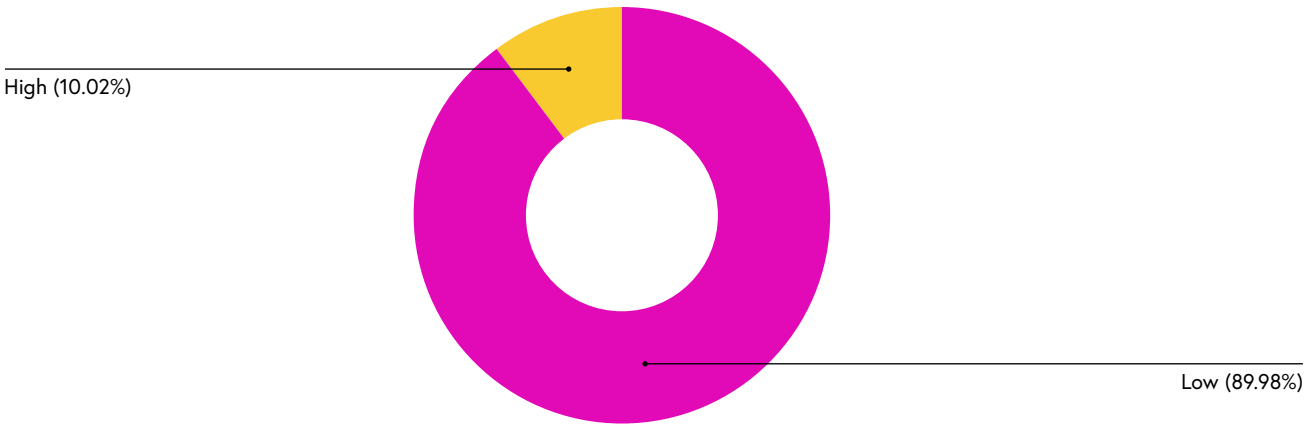


Figure 3.1c: Breakdown of attack complexity.

PRIVILEGES REQUIRED

This metric represents the level of privileges an attacker must have before successfully exploiting the vulnerability. As you can see in the following graph, for 76.39% of the vulnerabilities, the attacker is unauthorized prior to attack and doesn't require any access to settings or files of the target.

CVSS PRIVILEGES REQUIRED

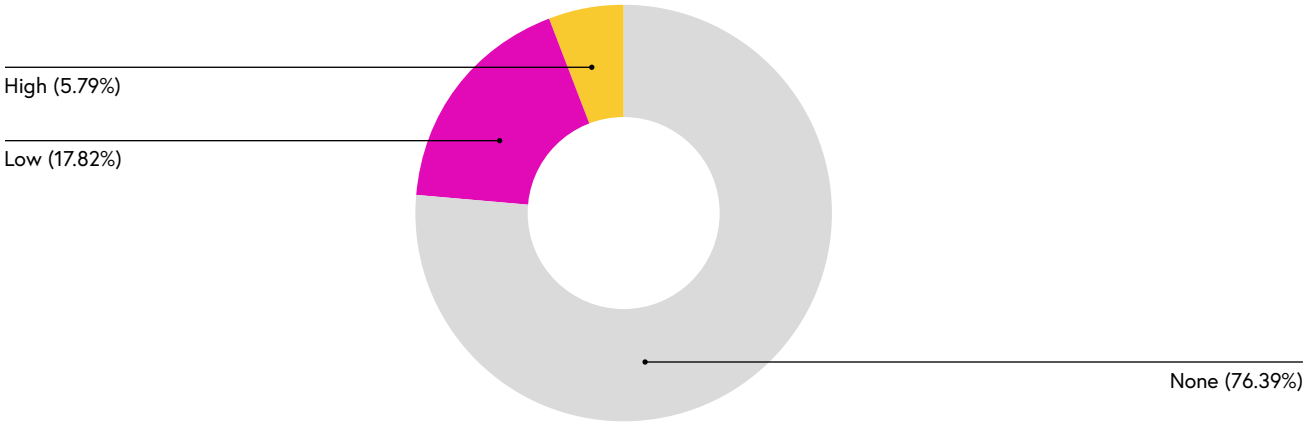


Figure 3.1d: Breakdown of privileges required.

USER INTERACTION

This metric represents whether an attacker depends on the participation of a seperate user or user-initiated process in order to exploit the vulnerability.

As you can see in the following graph, for 78.17% of the vulnerabilities, there is no requirement for user interaction.

CVSS USER INTERACTION

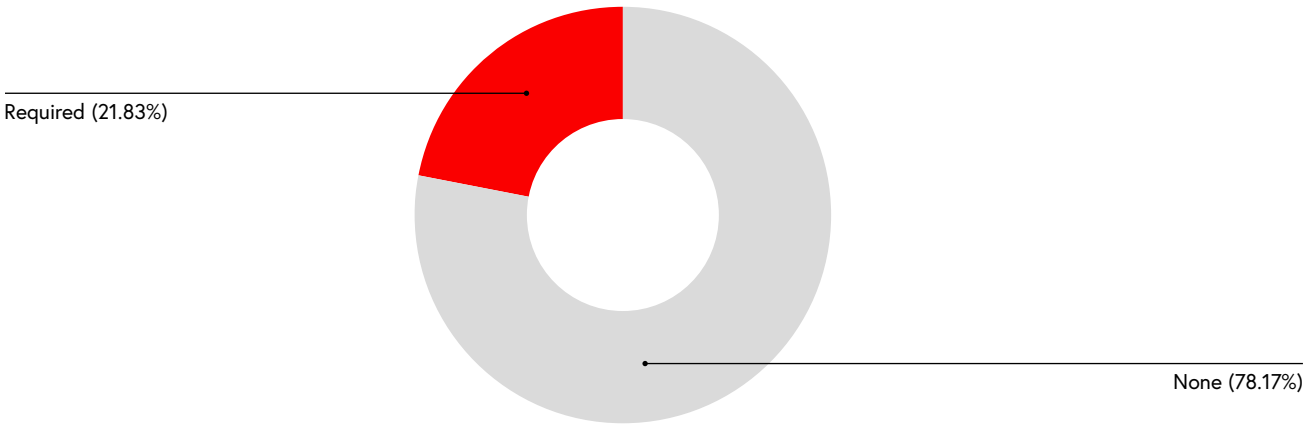


Figure 3.1e: Breakdown of user interaction required for exploitation.

IMPACT METRICS

These metrics represent the direct consequences of a successful exploitation of each vulnerability. The CVSS system measures impact according to the CIA triad (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. In the following sections, you can see the lesser relevance of confidentiality and integrity as risk variables in OT networks. Therefore, ICS defenders need to evaluate the severity of a vulnerability further than just its CVSS score.

CONFIDENTIALITY

This metric represents the impact to the confidentiality of the information resources as a result of successful exploitation of a vulnerability.

As you can see in the following graph, the impact to confidentiality is low or none for more than 94.43% of the vulnerabilities. This shows that, as mentioned above, while confidentiality is important in IT security, it acts as a far less significant risk variable in OT networks.

CVSS CONFIDENTIALITY

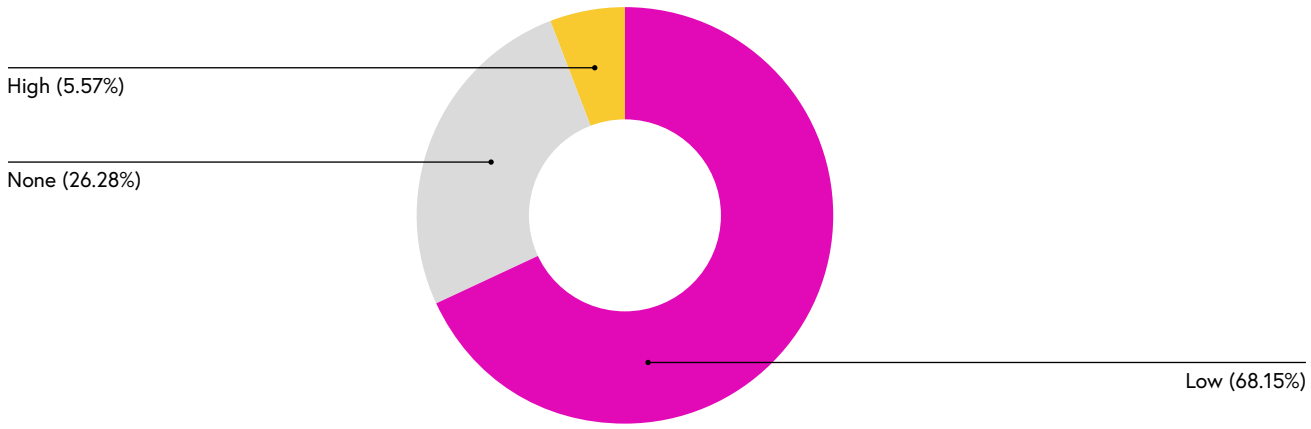


Figure 3.1f: Breakdown of confidentiality as an impact of ICS vulnerabilities.

INTEGRITY

This metric represents the impact to the integrity of information as a result of successful exploitation of a vulnerability. As you can see in the following graph, for 80.4% of the vulnerabilities, the impact to confidentiality is none whatsoever. Again, as mentioned above, it shows that while integrity of information is important in IT security, it acts as a lesser risk variable in OT networks.

CVSS INTEGRITY

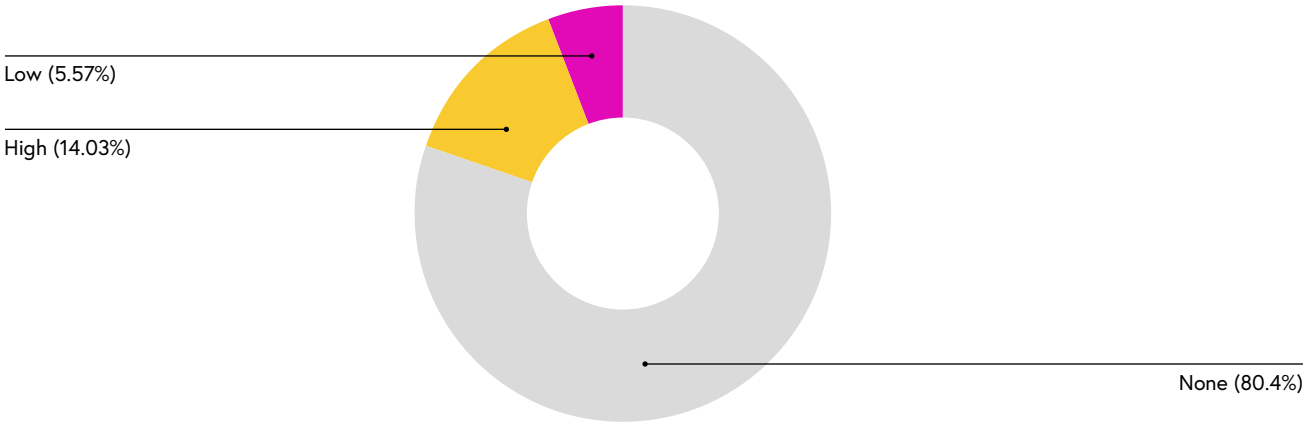


Figure 3.1g: Breakdown of integrity as an impact of ICS vulnerabilities.

AVAILABILITY

This metric represents the impact to the availability of the impacted component as a result of successful exploitation of a vulnerability. As you can see in the following graph, for 65.7% of the vulnerabilities, the impact to availability is high. This means there is total loss of availability, resulting in denial of access to resources. Alternatively, the loss of availability may be partial but significant—for example, denying the ability to create new connections.

CVSS AVAILABILITY

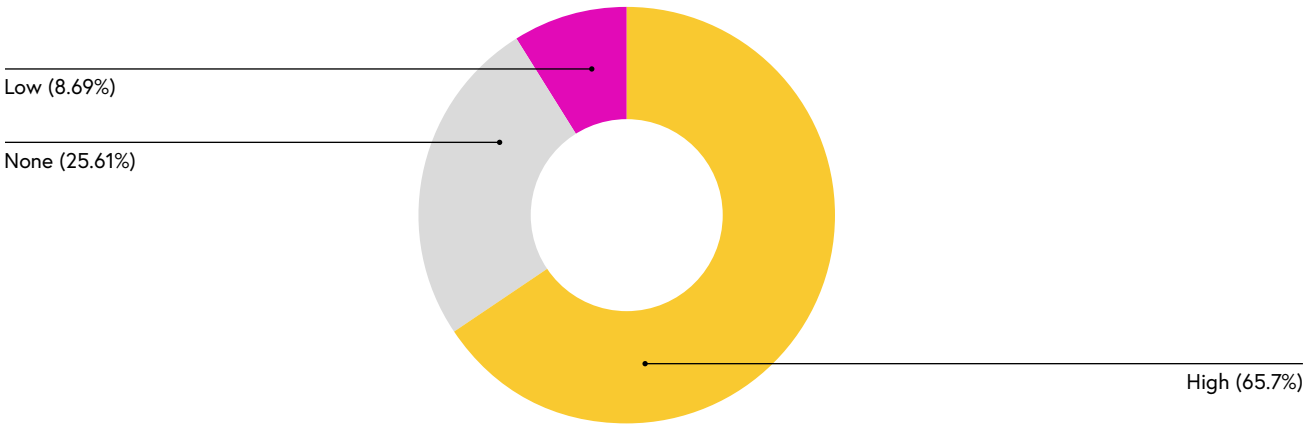


Figure 3.1h: Breakdown of availability as an impact of ICS vulnerabilities.

SCOPE

This metric represents whether a vulnerability in a component impacts sources in components outside of its "security scope." As you can see in the following graph, for 87.97% of the vulnerabilities, the scope is unchanged, meaning that these exploited vulnerabilities can only affect resources that are under the same security scope.

CVSS SCOPE

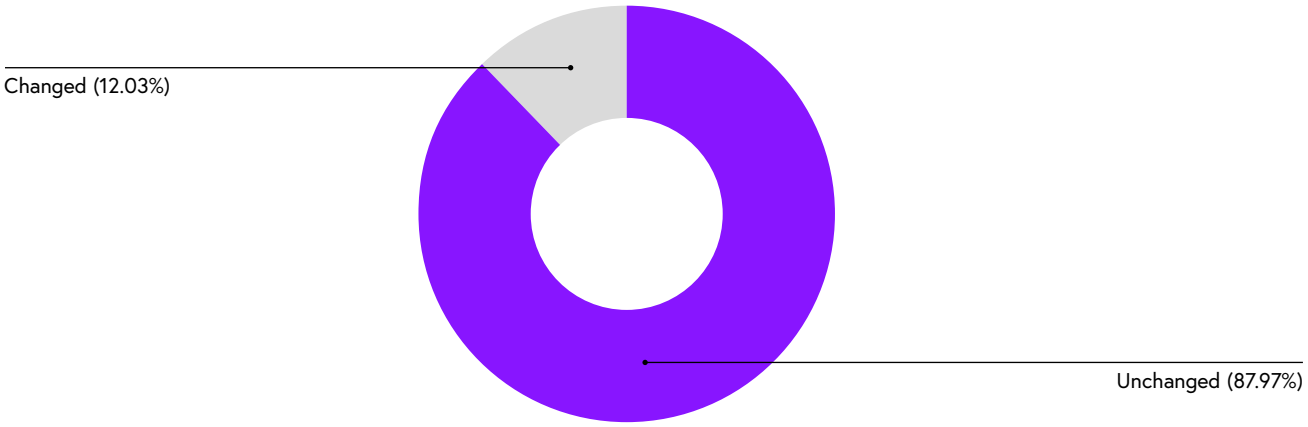


Figure 3.1i: Breakdown of scope as an impact of ICS vulnerabilities.

CVSS SCORE

All the metrics mentioned above are measured and calculated into a final CVSS score that represents the severity of the vulnerability. This range of scores is divided into four categories: low, medium, high and critical.

70.38% of vulnerabilities are classified as high or critical. 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.

It also coincides with the previous findings that the majority of vulnerabilities are not complex, don't require privileges or depend on user interaction, and may cause total loss of availability.

CVSS CATEGORY DIVISION

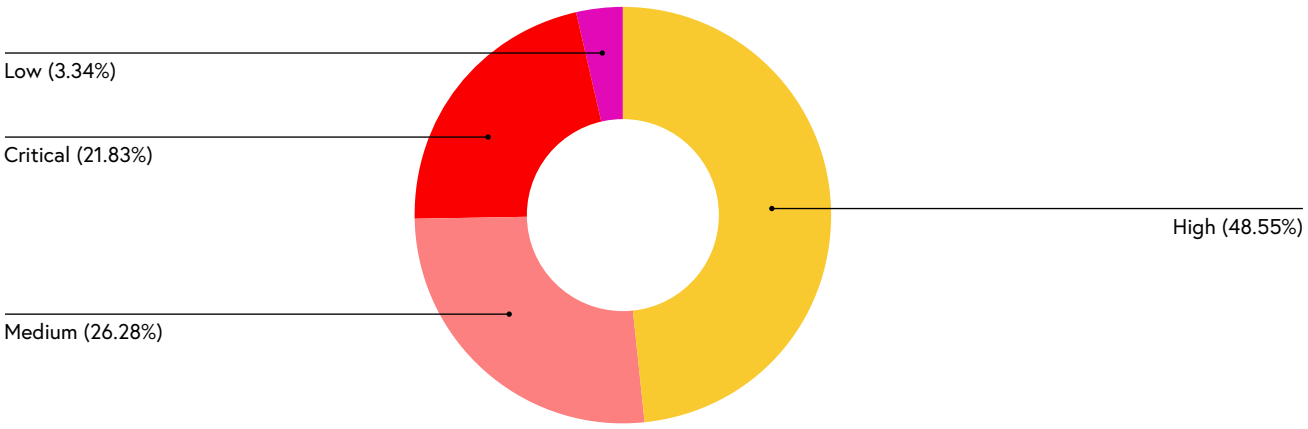


Figure 3.1j: Breakdown of CVSS criticality scores.

PART 4: EXPLOITED CWES

Security weaknesses—or Common Weakness Enumerations (CWEs)—manifested in the ICS vulnerabilities disclosed during 2H 2020 help explain why most of these vulnerabilities have CVSS scores categorized as either high or critical.

The top five most prevalent CWEs are all ranked highly on The MITRE Corporation's 2020 CWE Top 25 Most Dangerous Software Errors list due to their relative ease of exploitation and ability to enable adversaries to inflict serious damage.

These CWEs include:

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 6.74% of vulnerabilities, down from 10.97% in 2H 2019.
- This CWE is No. 2 on MITRE's 2020 Top 25 most dangerous software weaknesses.

CWE-125 OUT-OF-BOUNDS READ

The software reads data past the end, or before the beginning, of the intended buffer.

Successful exploitation can result in the ability to read memory and bypass protection mechanisms.

- This CWE manifests in 5.65% of the vulnerabilities, up from 1.79% in 2H 2019.
- This CWE is No. 4 on MITRE's 2020 Top 25 most dangerous software weaknesses.

CWE-79 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION (CROSS-SITE SCRIPTING)

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 mechanism, or ability to read application data.

- This CWE manifests in 4.57% of the vulnerabilities, up from 4.34% in 2H 2019.
- This CWE is No. 1 on MITRE's 2020 Top 25 most dangerous software weaknesses.

CWE-287 IMPROPER AUTHENTICATION

When an actor claims to have a given identity, the software does not prove or insufficiently proves that the claim is correct. Successful exploitation can result in ability to read application data, gain privileges or assume identity, code or command execution

- This CWE manifests in 4.57% of the vulnerabilities, down from 6.12% in 2H 2019.
- This CWE is No. 14 on MITRE's 2020 Top 25 most dangerous software weaknesses.

CWE-200 EXPOSURE OF SENSITIVE INFORMATION TO AN UNAUTHORIZED ACTOR

The product exposes sensitive information to an actor that is not explicitly authorized to have access to that information. Successful exploitation can result in the ability to read application data.

- This CWE manifests in 4.13% of the vulnerabilities, down from 5.87% in 2H 2019.
- This CWE is #7 on MITRE's 2020 Top 25 most dangerous software weaknesses.

POTENTIAL IMPACTS OF ICS VULNERABILITIES BASED ON CWE

The chart below depicts the most prevalent potential impacts of ICS vulnerabilities published during 2H 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, bypass protection mechanisms, or gain privileges and assume identity.

VULNERABILITY COUNT BY IMPACT

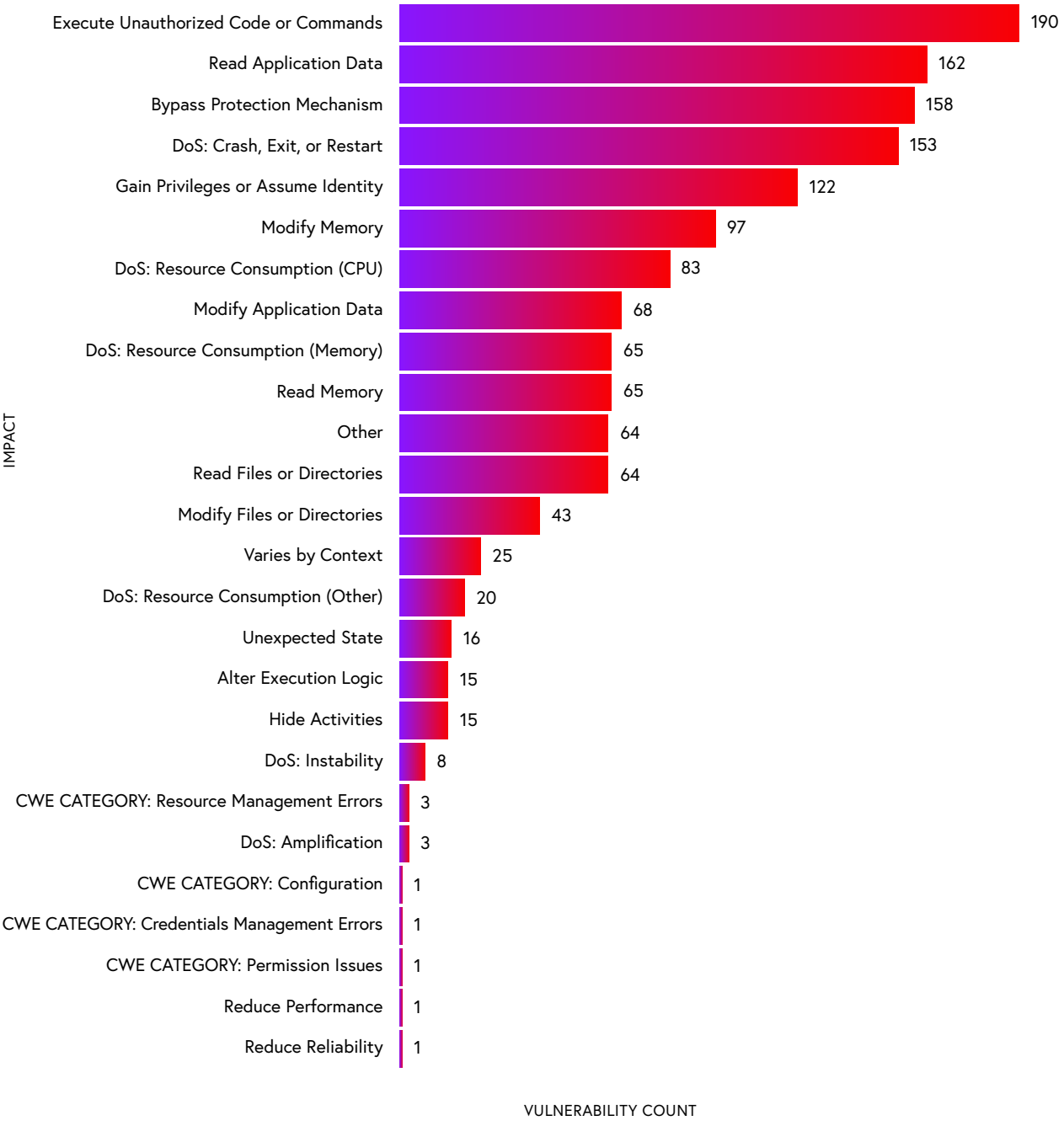


Figure 4.1: Breakdown of vulnerability counts by CWE impact.

A comparison of ICS vulnerability data from the 2H of 2018, 2019, and 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 2.06% from last year, but this figure still marks an increase of 55.74% since 2H 2018, while read-application data (+8.72%, +110.39%), bypass protection mechanisms (+32.77%, +135.82%), and DoS (+2%, +59.38%) all saw notable increases from 2H 2018.

Further down the list of potential impacts, gain privileges or assume identity increased by 31.18% since 2H 2019 and 100% since 2H 2018, making them the fifth most prevalent impact. Modify application data increased by 33.33% and 183.33%, and modify files and directories increased by 48.28% and 95.45%, respectively. These impacts could compromise the availability of impacted systems, hence the growing efforts of researchers to identify them.

YEAR-OVER-YEAR COMPARISON OF VULNERABILITY COUNT BY IMPACT TOP 15

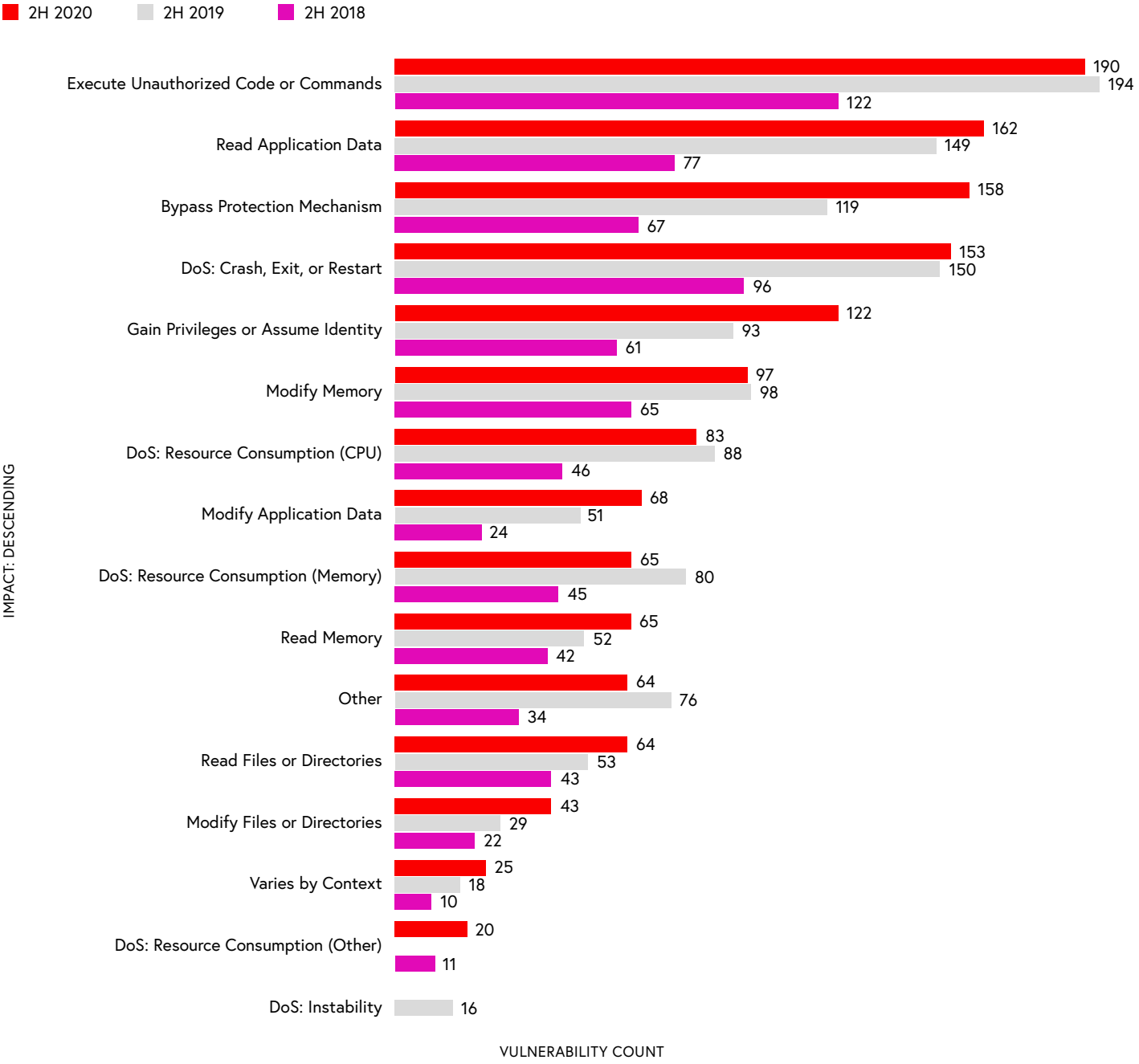


Figure 4.1b: Year over year comparison of vulnerability counts by impact.

PART 5: KEY EVENTS RELEVANT TO THE 2H 2020 ICS RISK & VULNERABILITY LANDSCAPE

Criminal and nation-state cyber activity, geopolitical events, and global crises served to shape the ICS risk and vulnerability landscape in 2020. 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.

The Claroty Research Team assesses that the following events and trends likely helped shape the ICS risk and vulnerability landscape to a degree during the 2H 2020.

5.1 EXTORTION AND RANSOMWARE ATTACKS AGAINST HEALTHCARE

As mentioned in the previous biannual report, there has been a rise in cyberattacks since the start of the COVID-19 pandemic, as opportunistic threat actors have sought to take advantage of the global health crisis.

Adversaries recognize that since healthcare providers are a vital necessity—particularly during the pandemic—they simply cannot afford to lose access to their critical systems, and thus tend to be more likely to pay ransoms. During the course of 2H 2020, the healthcare sector experienced multiple waves of ransomware attacks targeting hospitals in the U.S and Europe. To that end, and the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory regarding ransomware attacks targeting the healthcare sector warning of this risk in late October.

As was seen in an attack on the IT network of a German hospital, targeted ransomware attacks against the healthcare sector can have devastating effects. The Duesseldorf University Clinic's systems gradually crashed and there was no access to data, leading to emergency patients being taken to other medical centers and surgeries being postponed. Officials tried to link the attack to the death of a woman in need of emergency treatment after she had to be taken to a hospital in another city for treatment.

Of course, ransomware can cause damage to hospitals even when they are not the actual target. As was seen in 2017, during which WannaCry spread across the world and infected the U.K's National Health System, disrupting operations at more than 80 medical facilities.

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

5.2 WIBU-SYSTEMS' CODEMETER VULNERABILITIES

Claroty researchers discovered six critical vulnerabilities in Wibu-Systems' CodeMeter third-party license-management component, affecting products sold by multiple vendors, including Siemens, Schneider Electric, and Rockwell Automation.

The vulnerabilities could expose users in numerous industries to a takeover of their OT networks and be exploited via phishing campaigns or directly by attackers, who are able to fingerprint user environments in order to modify existing software licenses or inject malicious ones, causing devices and processes to crash.

Furthermore, Claroty researches also discovered encryption implementation issues, which can be exploited to allow attackers to execute code remotely and move laterally on OT networks.

The vulnerabilities would allow an attacker that is either performing a phishing campaign or already has network access to engineering stations and HMIs in critical environments, enabling them to completely take over those hosts running ICS software from many of the leading vendors. This means the attacker could impact and modify physical processes (as was done in the Triton attacks using Industroyer) or install ransomware, as was alleged in the recent incident affecting Japanese automaker Honda, thus effectively taking down the ICS environment.

Wibu-Systems has made patches available for all of the flaws in version 7.10a of CodeMeter, which has been available since Aug. 11.

For further information regarding CodeMeter vulnerabilities refer to:
https://www.claroty.com/2020/09/08/blog-research-wibu-codemeter-vulnerabilities/

For further information regarding affected vendors refer to:
https://claroty.com/2020/09/08/blog-research-vendors-affected-by-wibu-codemeter-vulnerabilities/

5.3 ZEROLOGON VULNERABILITY IN MICROSOFT NETLOGON

A critical vulnerability called Zerologon was discovered in Netlogon, a service within Microsoft Active Directory, which is used to manage domains and users, as well as authentication and authorization to network assets.

Zerologon allows an attacker to escalate privileges in a domain environment, taking advantage of an insecure AES-CFB8 cryptographic algorithm implementation. The ComputeNetlogonCredential function in Netlogon uses a fixed initialization vector consisting of 16 bytes of zeros, rather than a randomized one. This means that an attacker could control the deciphered text and then impersonate any machine on a network authenticating to the domain controller (DC), including the domain administrator Active Directory is often installed in an OT network or used cross-domain between IT and OT networks. Technologies such as distributed control systems (DCS), for example, may be particularly vulnerable to this bug, because they often rely on AD as their main authentication repository for network credentials. Penetrating the domain controller of an industrial network could put an attacker in position to interfere with and damage business processes.

Energetic Bear, an APT actor against U.S. state, local, territorial, and tribal (SLTT) government networks—as well as aviation networks—has been exploiting the unpatched Zerologon vulnerability to access Active Directory servers and elevate privileges in order to move laterally across compromised networks. The group, which has been linked to Russian intelligence, has targeted organizations in the oil and gas industry in the west for years.

Microsoft made a patch available for CVE-2020-1472 as part of a phased two-part rollout. Part two of the rollout will be available in the first quarter of 2021.

For further information regarding the Netlogon vulnerability, refer to:
https://claroty.com/2020/09/17/blog-research-patched-netlogon-flaw/

For further information regarding Energetic Bear's targeting of Zerologon, refer to:
https://claroty.com/2020/10/27/blog-research-energetic-bear-zerologon/

5.4 AMNESIA:33 VULNERABILITIES

AMNESIA:33 is a set of 33 vulnerabilities impacting four open source TCP/IP stacks (uIP, FNET, picoTCP, and Nut/Net) discovered and disclosed by Forescout Research Labs.

The vulnerablilites affect seven different components of the stacks mentioned above: DNS, IPv6, IPv4, TCP, ICMP, LLMNR and mDNS. Two vulnerabilities in AMNESIA:33 only affect 6LoWPAN wireless devices.

The TCP/IP stacks affected can be found in operating systems, embedded devices, systems-on-a-chip, networking equipment, OT devices, and a myriad of consumer and enterprise IoT devices. As often happens with third-party vulnerabilities, the scope of affected devices and vendors is unclear and is being updated on an ongoing basis.

Successful exploitation can potentially lead to code execution, DoS via crash or infinite loop, information leak, and DNS cache poisoning. An attacker can take full control of a target device, harm functionality, obtain sensitive information, or inject malicious DNS records that will point devices to a domain controlled by the attacker.

Some of the stacks' mainterners released version updates, but it is important to take notice of the fact that some of the TCP/IP stacks are end-of-life.

For further information regarding affected vendors, devices, and recommendations, refer to:
https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01

5.5 SUPPLY-CHAIN ATTACKS

As we assess the ICS risk and vulnerability landscape, we mostly focus on vulnerabilities and weaknesses within OT networks which, upon exploitation, the attacker can achieve a certain effect. But when taking a step back from the production environment, we identify another risk: what if the industrial control system is exploited before it's even in production? That is where supply chain attacks enter the picture.

Supply chain attacks occur when an attacker infiltrates your system through an outside provider or partner, and they span the lifecycle of a product:

Design › Manufacturing › Distribution › Storage › Maintenance

In every single one of these steps, there is a risk of an attack targeting the less secure elements in the chain. This risk complicates the situation, because the process is not necessarily done entirely in one geographical area or under the responsibility of a single organization.

In the last decade, awareness of supply chain attacks grew as major incidents were reported. For example, in the Target security breach (2013), attackers used stolen credentials from the vendor that provided the HVAC systems in Target stores in order to access its network and move laterally until finally stealing bank card and personal information of millions of customers, resulting in hundreds of million of dollars in damages for the retailer.

The NotPetya ransomware (2017) was also a supply chain attack, as the attackers first compromised M.E.Doc, a Ukraininan accounting firm, poisoning its software updates that were downloaded by victims, allowing NotPetya to spread around the world. NotPetya affected multinational corporations such FedEx, Merck, and Maersk, ultimately causing an estimated $10 billion in damages, making it one of the most expensive cyber attacks to date.

Most recently, a supply chain attack trojanizing SolarWinds Orion software was discovered. This attack was used to distribute the SUNBURST backdoor. The attack allowed a threat actor to gain access to numerous organizations around the world as part of SolarWinds' software update process. The campaign was closed by Microsoft, but the full extent of the attack's reach and damage is yet to be known.

Finally when thinking about COVID-19, the pandemic that very well shaped security risks and cyber attacks during 2020, we must also take the vaccines' supply chain into consideration.

For further information regarding OT supply chain risk, refer to:
https://blog.claroty.com/understanding-and-defending-against-ot-supply-chain-risk

PART 6: THINGS TO FOCUS ON IN 2021

After a painful 2020 that affected the ICS risk and vulnerability landscape around various industry sectors, there is no doubt that the consequences will start to emerge in 2021.

FALLOUT OF COVID-19

During 1H 2020, lockdowns and shelter-in-place mandates enacted in light of COVID-19 required companies globally to find remote alternatives for their employees resulting in an increase of remote workers.

- Working from home continued in 2H 2020 as well, and created security gaps and expanded the attack surface for many organizations lacking secure remote access solutions.
- Decreased on-site work delayed deployment of new equipment and upgrades of existing ones.

Taking advantage of the situation, adversaries that targeted remote workers could get access to enterprise networks and OT networks.

RANSOMWARE

Ransomware is on the rise, and many ransomware strains are being modified on an ongoing basis to include modules that:

- Steal sensitive data to enable extortion
- Drop malware
- Locate valuable assets in the network
- Target specific equipment or OS

Ransomware is also popular against critical infrastructure sectors that cannot afford downtime and may be more likely to pay the ransom. It is likely that during 2021, we will see more ransomware attacks affecting critical sectors, employing extortion methods, and strategic targeting.

MOVING TO THE CLOUD

As digital transformation steams ahead, industrial organizations are also looking at the cloud for efficiencies, especially around reducing infrastructure costs. Operationally, a number of standardized OT protocols already allow for the exchange of data with cloud-based providers that host platforms or infrastructure necessary to maintain an OT network. Development and processing power are attractive cloud offerings, but businesses must do so securely to avoid introducing additional risks.

This means enforcing authentication and strong encryption to prevent illicit access to systems and data. The cloud can also be a key part of a company's network segmentation strategy for OT, much in the same way it has for IT operations. Many important cloud technologies around virtualization that have been staples in IT may also be crucial to the security and reliability of OT networks.

PART 7: RECOMMENDATIONS

PROTECTING BASIC & SUPERVISORY CONTROL

The majority of the vulnerabilities disclosed during 2H 2020 affected Level 2-Supervisory Control (HMIs, SCADA and engineering stations), followed by the Level 1-Basic Control (controllers, PLCs, RTUs).

Most of the Supervisory Control vulnerabilities are software based, compared to Basic Control, where the majority are firmware based. With the inability to patch over time, especially level 1 device firmware, it is recommended to invest in segmentation, remote access protection, and better protection of the Supervisory Control level, because it provides access to the Basic Control level, and eventually, the process itself. Other recommendations include:

- Secure remote access connections using mechanisms such as encryption, access control lists, and appropriate remote access technologies suitable for OT networks.
- Maintain asset inventory and segmentation.
- Assess risks and prioritize critical patches.
- Ensure the devices are password-protected and that stringent password hygiene is enforced.
- Implement granular role- and policy-based administrative access.
- As we saw that the majority of the local attack vector based level 2 vulnerabilities were dependent on user interaction adhere to best practices below against social engineering techniques.

RANSOMWARE, PHISHING, AND SPAM PROTECTION

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 email 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 (sensitive information is also used for extortion).
- 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.

THIRD-PARTY VULNERABILITIES

As organizations depend more and more on third-party solutions to get work done, it becomes increasingly difficult to ignore the security issues that stem from this reliance. Over the course of 2020, there have been disclosures of numerous third-party vulnerabilities affecting numerous products from multiple vendors in various industry sectors, including CodeMeter, Netlogon, Ripple 20, and AMNESIA:33.

While these disclosures demonstrate the potential damage of widespread security issues affecting the entire ICS domain, they also showcase the difficulty of protecting and mitigating against these vulnerability types.

As security practitioners take on this challenge, the following steps should be taken into account:

- Visibility: The first step is to know what third-party components exist across the various assets within the OT network.
- Risk Assessment: Identify potential risks in usage of these third-party components.
  - Start by inspecting existing security issues of the third-party components and their impact
  - Determine if the component will be end-of-life within the lifecycle of the product
  - Assess the maturity of the components' provider in terms of maintenance and stability
- Risk Mitigation
  - Use patched versions; this may be difficult because of the inability to patch in OT networks as frequently as in IT networks. If a component is end-of-life, updates should be done when possible
  - Implement input validation and output sanitization in embedded products
  - Reduce privileges of "external" code of the third-party component
  - Use hardening methods: for example, disable unnecessary services
- Monitoring: Monitor different public sources such as vulnerability databases or the third-party providers' security advisories continuously to discover new vulnerabilities or components reaching end of life.

SUPPLY CHAIN VULNERABILITIES

The SolarWinds attack has again put defenders' focus back on the supply chain. Organizations need more scrutiny on their partners, contractors, vendors, and other entities with credentialed access to internal systems, or manufacturers of hardware and firmware they may be purchasing.

Managing this critical risk starts with determining internal responsibility for procurement and verifying a partner's process security. This requires legal teams to be involved, in addition to technology and line-of-business leaders across business units and geographies. Decision makers need threat intelligence related to supply chain attacks in order to make informed decisions about risks to the business. Secure procurement and data protection must be wrapped in effective communication with partners and internal stakeholders.

As 2021 progresses, there will be no more important industrial supply chain than the COVID-19 vaccines. The massive undertaking of efficiently manufacturing and distributing the vaccine safely across the globe is an issue that requires preparation. Given the unprecedented criticality of current circumstances, organizations involved at each step of the vaccine's supply chain must focus on operational security in order to ensure the reliability and safety of the product:

- Detailed Operational Visibility: Organizations need a dedicated security solution capable of overcoming OT-specific challenges, which include a lack of standardized technology, the use of proprietary protocols, and a low tolerance for disruptions to critical processes.

- Consistent Cybersecurity Standards: Adhere to the industry-specific recommendations detailed in the July 23 CISA alert, which can help mitigate increased cyber risk driven by growing connectivity of OT assets to the Internet across all 16 U.S. critical-infrastructure sectors.

- Strengthened Cybersecurity Coalitions: Given the critical urgency of the current moment, many executives and board members have become attuned to operational concerns, and are therefore more aware of why having the right cyber defense technology and processes in place is essential for ensuring availability, reliability and safety. As such, there has never been a better time for CISOs and other security leaders to garner cross-functional buy-in for supporting present and future industrial cybersecurity initiatives.

For further information regarding securing the COVID-19 vaccine supply chain, refer to:
https://claroty.com/2020/12/07/blog-covid-19-supply-chain/

DEFENSE-IN-DEPTH

Based on latest alerts by CISA, publicly facing services are a growing target. For example, Russian state-sponsored actors exploited a VMware vulnerability that allowed them access to protected data on affected systems.

Access to sensitive organizations that started in 1H, while taking advantage of the high usage of remote access solutions as a result of COVID-19, transitioned into supply chain attacks (SolarWinds). These circumstances showcase that a single line of defense is not enough, and security should be applied in depth to avoid a single point of failure.

Asset owners should invest in network detection based solutions, secure remote access systems, internet facing devices protection, and other security measures suited to their industrial environments. To be effective, these investments must be incorporated into a layered defense strategy within their organization's network.

ACKNOWLEDGEMENTS

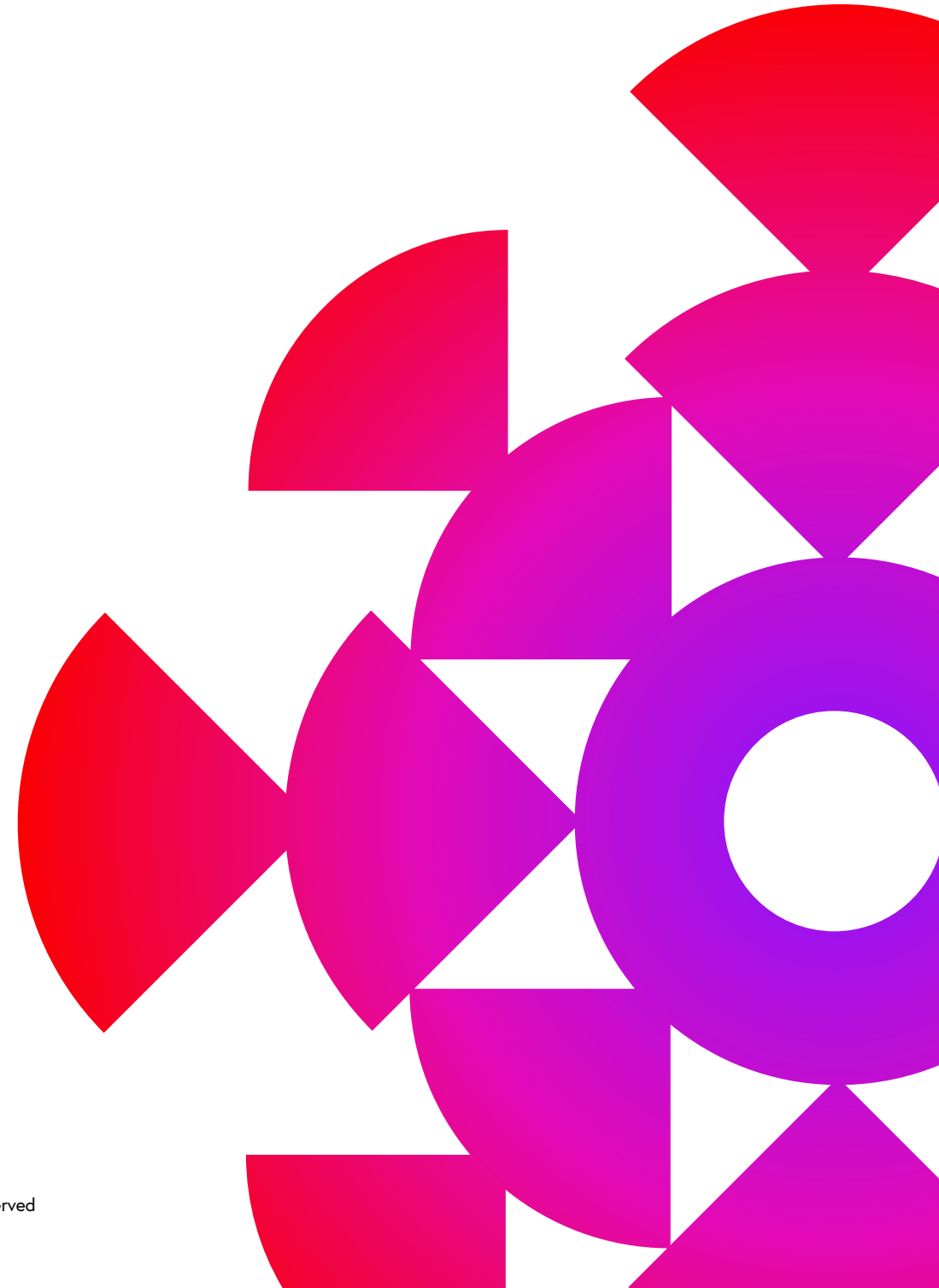
The primary author of this report is Chen Fradkin, security researcher at Claroty.

Contributors include: Rotem Mesika, security research team lead at Claroty, Nadav Erez, director of innovation, Sharon Brizinov, vulnerability research team leader, and Amir Preminger, vice president of research at Claroty. Special thanks to the entire Claroty Research Team for providing exceptional support to various aspects of this report and research efforts that fueled it.

ABOUT CLAROTY

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America, and deployments on all seven continents.

To learn more, visit www.claroty.com.



CLAROTY