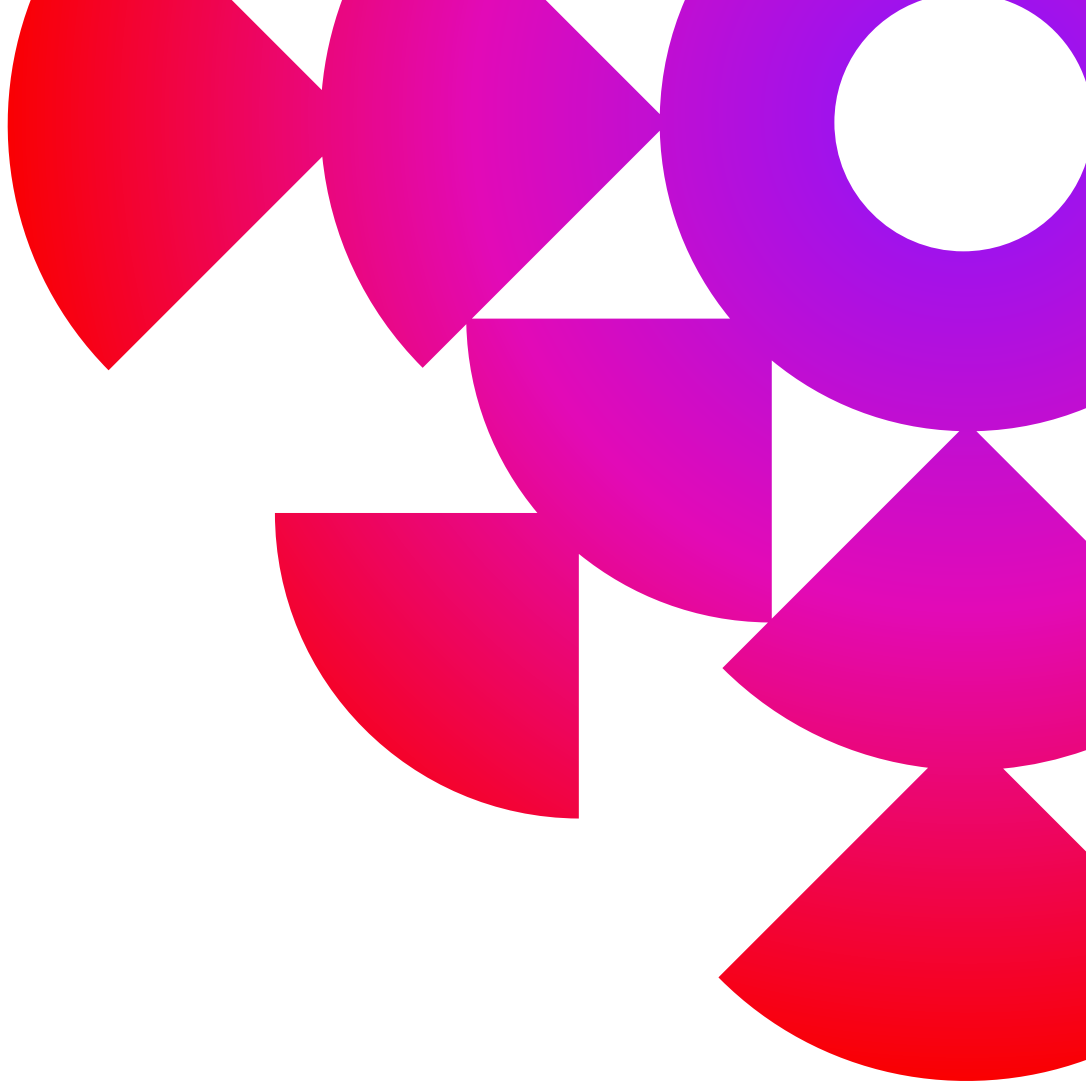


CLAROTY BIANNUAL ICS RISK & VULNERABILITY REPORT: 2H 2021

By Claroty Team82

CLAROTY

CONTENTS

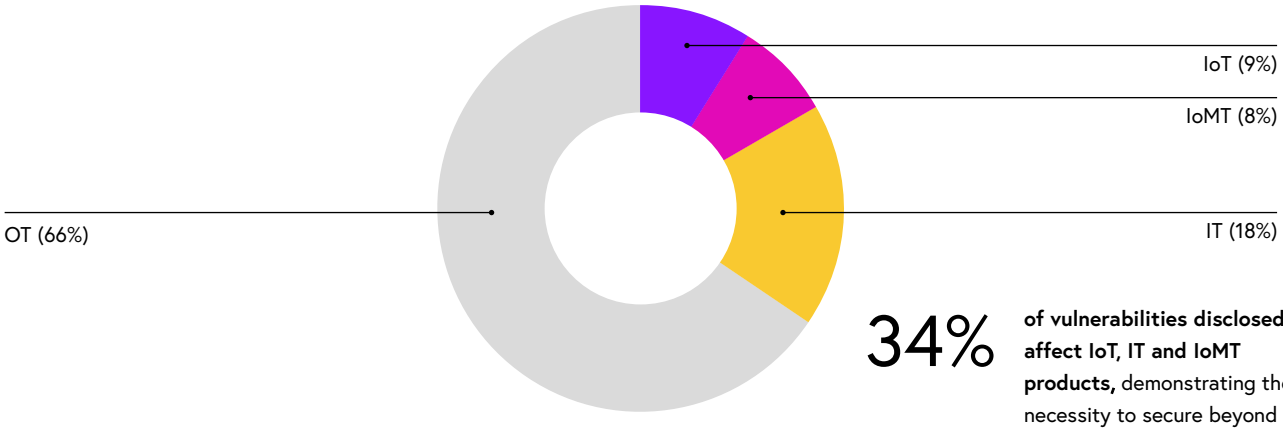
EXECUTIVE SUMMARY

We are fast approaching a time when highly connected cyber-physical systems are the norm, and the lines between information technology (IT), operational technology (OT), and Internet of Things (IoT) security management are blurred.

All of it will be connected to, and managed from, the cloud, and unfathomable amounts of data will be processed in order to fine-tune performance, deliver analytics on key services, and ensure the integrity of critical industrial, healthcare, and enterprise processes.

This is the new paradigm of the Extended Internet of Things (XIoT), one that enhances the need for timely, useful vulnerability information in order to better inform risk decisions. Claroty, today, publishes its fourth Biannual ICS Risk & Vulnerability Report. The report was prepared by Claroty's research arm, Team82, in effort to define and analyze the vulnerability landscape relevant to leading automation products and connected devices used across domains.

While the volume of headline-grabbing attacks dwindled in the second half of 2021 compared to the first six months, those incidents will only fuel the eventual prioritization of XIoT cybersecurity among decision makers. You'll also see from our analysis in this report—our data sources encompass all commercial products running inside critical infrastructure and other sectors such as manufacturing, healthcare, and IoT—that the percentage of vulnerabilities that were disclosed in the second half of last year in connected IoT and medical devices, as well as a growing number of IT vulnerabilities, continues to climb, reaching 34%, up from 29% in 1H 2021.



34% **of vulnerabilities disclosed affect IoT, IT and IoMT products,** demonstrating the necessity to secure beyond OT to the XIoT.

Digital transformation and converged ICS and IT infrastructures are also pushing researchers who once purely focused on OT to extend their work to XIoT.

Note: Team82's rounding up of percentages accounts for the totals in this graphic exceeding 100%.

This indicates that organizations will merge OT, IT, and IoT under converged security management, and that OT and ICS will no longer be their own walled-off disciplines. Therefore, asset owners and operators must have a thorough snapshot of their environments in order to manage vulnerabilities and lessen their exposure.

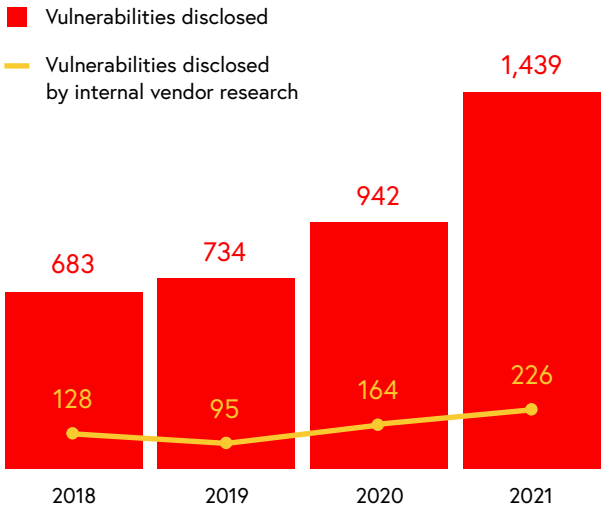
In this report, Team82 delivers a comprehensive look at industrial control system (ICS) vulnerabilities publicly disclosed during the second half of 2021, including those found by Team82 and those found by affected vendors, independent security researchers, and experts inside other organizations.

Security managers, asset owners, and operators, are urged to use this report as a resource, one that delivers not only data about vulnerabilities that are prevalent in industrial devices, but also the necessary context around them to assess risk within their respective environments.

Let's look at some key data points from the Biannual ICS Risk & Vulnerability Report: 2H 2021:

SECURITY RESEARCH AND DISCLOSURE TRENDS

- During 2H of 2021, **797** ICS vulnerabilities were published, affecting **82** ICS vendors. **21** of these vendors are newly affected and had no recently published disclosures. Most of those **21** vendors were in automation, manufacturing, and healthcare.
- Team82 disclosed **110** vulnerabilities during the 2H 2021 affecting **16** automation vendors. Since its inception, Team82 has found and reported more than **260** vulnerabilities to affected vendors.
- Data shows an increase in ICS vulnerability disclosures and the number of vulnerabilities disclosed by internal research done by vendors. Coincidentally the amount of vendors doing internal research increased by **35%**.

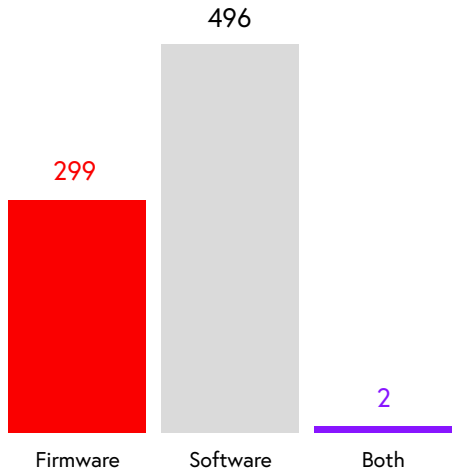


+110% **Increase**
in vulnerabilities disclosed

+76% **Increase**
in number of vulnerabilities disclosed by internal vendor research.

- Siemens was the vendor with the most reported vulnerabilities at **251**, thanks to its internal research conducted by the Siemens ProductCERT. Schneider Electric, Advantech, Delta Electronics, and Mitsubishi were the next most affected vendors.

- In 2H 2021, the majority of vulnerabilities affect software components, right, and given the comparative ease in patching software over firmware, defenders have the ability to properly prioritize patching within their environments.

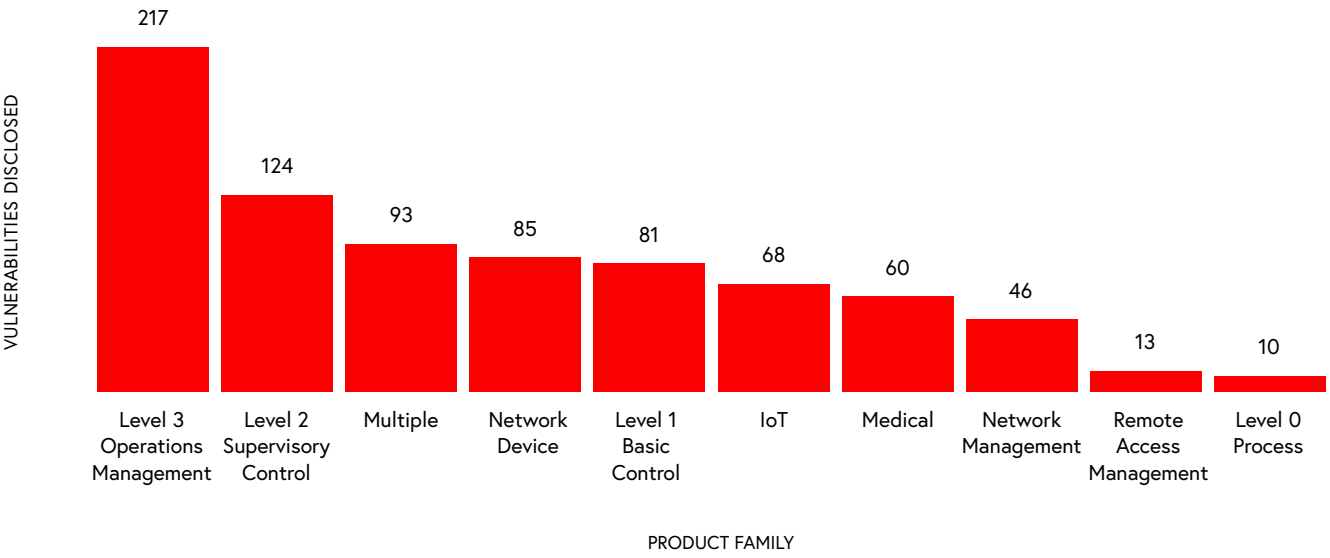


THREATS AND RISKS FROM ICS VULNERABILITIES

- For the second straight report, products fitting within Operations Management—Level 3 of the Purdue Model—were the most affected by disclosed vulnerabilities, see chart, below. The software components at this level include the servers and databases at the core of the production workflow. Technology at this level also feeds data collected from field devices to higher-level business systems, or those operating in the cloud.

  Products operating at the Basic Control (Level 1) and Supervisory Control (Level 2) levels were affected by 25% of the vulnerabilities disclosed in the 2H 2021 (205 combined). At the Basic Control level are programmable logic controllers (PLCs), remote terminal units (RTUs), and other controllers that monitor Level 0 equipment such as pumps, actuators, sensors, and more. At the Supervisory Control level are human-machine interfaces (HMIs), SCADA software, and other tools that monitor and act on Level 1 data.

AFFECTED PRODUCT FAMILIES



Defenders must understand what threat vectors are most exploited by attackers targeting industrial networks and IoT devices. Proper visibility into where vulnerabilities are found allows organizations to adequately patch or mitigate issues in software and firmware putting networks and processes at risk.

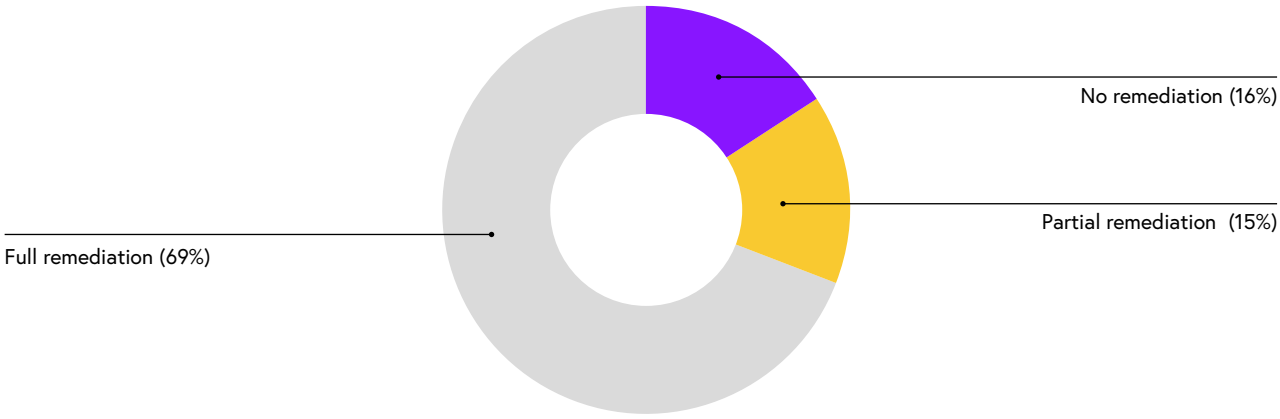
Remotely Exploitable Vulnerabilities: Team82's data shows that 63% of the vulnerabilities disclosed may be exploited remotely through a network attack vector. That number is up slightly (2%) from 1H 2021.

Local Attack Vectors: The percentage of locally exploitable vulnerabilities dropped in the 2H 2021 to 31%. To exploit these vulnerabilities, an attacker would need a separate vector for network access in order to exploit these flaws; some of those would require user interaction, such as phishing and spam to gain that initial network foothold.

- Digging further: **94%** of operations management disclosures via a local attack vector require user interaction for exploitation, reinforcing the need for continuous education to prevent phishing attacks and stem the tide of destructive ransomware attacks, for example.

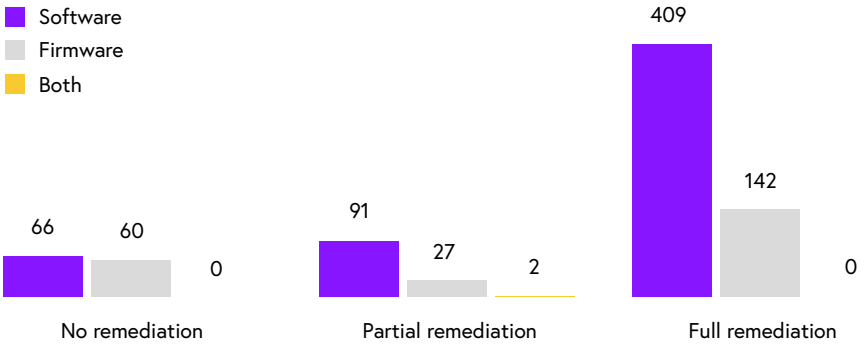
Disclosing vulnerabilities is only one, albeit crucial, step in the vulnerability management process. Patches and mitigations are of utmost importance to asset owners, operators, and security managers. With more connected devices coming online every day, an increasing number of systems are reachable and escalate the urgency for prompt fixes.

Mitigations and Remediation: Updating ICS or SCADA software is often challenging for a number of well-understood reasons, largely having to do with uptime and availability requirements. Firmware updates are also difficult because of the complexity involved in developing and implementing updates. These cycles can take significantly longer than traditional IT patch management, often making mitigations the only remediation option open to defenders. Vendors and internal security analysts and managers must also prioritize tracking of vulnerabilities in end-of-life products and in products where updates may be challenging or downtime is unacceptable. The shelf life of ICS products is long, and as vulnerabilities—especially critical remote code execution or denial-of-service—accumulate, risk is amplified significantly.



Team82's data correlates with these trends:

REMEDIATION BY FIRMWARE/SOFTWARE



74% **of fully remediated vulnerabilities** are software-based. Emphasizing that given the comparative ease in patching software over firmware, defenders have the ability to prioritize patching within their environments.

62% **of partially or unremediated vulnerabilities** when exploited, could result in remote code execution or in denial-of-service

- Most of the fully remediated vulnerabilities were in products at the Operations Management level of the Purdue Model, followed by Supervisory Control, and network management.
- Fewer remediations exist for firmware. When they are provided by an affected vendor, firmware updates for network devices are addressed most frequently, followed by products at the Basic Control level, and IoT devices.
- End-of-life products are prevalent within industrial settings, and most organizations are hesitant to rip out legacy systems that oversee key processes. Team82's data shows there were 29 vulnerabilities affecting end-of-life products for which there is no remediation planned. In all cases, the affected vendors no longer support these products.
- 48% of vulnerabilities in end-of-life products affect Basic Control devices (PLCs, RTUs). Close to 60% of these flaws, if exploited, would crash an affected device.

TRENDS TO WATCH

CLOUDY FORECAST: SECURING XIoT

The Extended Internet of Things (XIoT) is an umbrella term that captures the cyber-physical systems critical to our lives. Connected devices, operational technology, healthcare systems, and much more are rapidly connecting online and to the cloud, not only for security management, but for data analysis, performance tracking and enhancement, and much more.

Those efficiencies are appealing to line-of-business owners, and it's the job of asset owners and security teams to secure those connections. This is a challenge on many fronts.

Team82 has been proactive about researching vulnerabilities in cloud-managed OT devices and not only how those devices may be impacted, but also management consoles in the cloud. This can be an alarming gap for enterprises connecting XIoT to the cloud.

A compromise of the management console is straightforward to understand: Exploit a vulnerability in the cloud and you have access to all the accounts and devices it manages. An attacker could then execute any number of exploits to run code on devices managed from the cloud, which enables not only full control of an endpoint device, but also lateral network movement and use of a greater array of payloads at their disposal. Likewise, Team82 has already demonstrated that it's possible to exploit a vulnerable device such as a cloud-managed PLC and eventually take over the cloud-based host account.

These types of top-down, bottom-up attacks are novel, and have been demonstrated as effective. They threaten process integrity by putting field devices such as PLCs at risk, and they also threaten data integrity and whether organizations can trust the data uploads devices are sending back to the cloud.

Managers overseeing converged XIoT environments must consider a range of potential weaknesses and how they can be exploited remotely or locally. The security of third-party partners such as vendors and suppliers must also be managed; a compromised vendor with access to sensitive systems is essentially a backdoor to cloud-managed systems. Multi-tenant hosts are also a risk to cloud-based XIoT systems. An attacker with access to the host system managed by a service provider would theoretically be able to target any of the virtual instances on that host, creating a single point of failure.

This is the risk management equation in front of XIoT operators and owners in 2022, who must weigh the risks of putting OT, IoT, and medical device management in the cloud against the business and operational benefits of doing so.

A FRAGILE SUPPLY CHAIN AND HOW SBOMS HELP

While SolarWinds was a jolt to technology owners and operators in early 2021, the critical vulnerability in Log4j disclosed in December demonstrated how fragile the software supply chain is, and how exploitable vulnerabilities in an open-source component can put thousands of companies and users at risk in an instant.

Log4j, a popular open source Apache logging framework, contained a remote code execution flaw that was trivial to exploit; Log4j is used by more than 2,000 companies, the Apache Software Foundation said. A malicious string that is logged by an application using Log4j triggers a JNDI (Java Naming and Directory Interface) lookup that would connect to an attacker-controlled server and load malicious Java code.

Automation vendors, like many others, use Log4j as a component across the OT domain putting numerous industrial processes at risk. While Log4j was quickly patched, equally as important were the resulting discussions about the software supply chain, and ensuring the secure use of open source components within critical infrastructure. CISA has compiled a list of affected vendors.

Secure software development has been a rallying point for many years, yet bringing security to developers has generally been viewed as an impediment to meeting deadlines and pushing new applications and code updates out the door.

A U.S. government Executive Order last year that was executed in the 2H 2021 specifically called out enhancements to the security of the software supply chain. The order made it clear that commercial software lacked transparency and resilience to attack, and demanded additional controls to prevent exploitable vulnerabilities from being introduced into code.

In addition to ensuring auditing trust relationships, requiring multi-factor authentication, encryption, and incident monitoring, the order insisted on supply chain providers making a software bill of materials (SBOM) available to organizations. SBOMs list out software components—including open source tools—used to build and compile commercial products; they are akin to ingredient lists on food labels.

Too often, organizations are blind to what makes up a popular piece of commercial software, and when a vulnerability in a component such as Log4j is disclosed, security teams scramble to determine their exposure and prioritize patch management processes. However, if an SBOM is made available, users can conduct not only vulnerability analysis, but also license analyses that help evaluate risks in products. Machine-readable SBOMs are important as well, and allow for integration into tools that enable them to be queried by applications and systems.

Expect supply chain security to remain a front-and-center risk management discussion in 2022, and SBOMs to be a critical component of those discussions.

A NEW RANSOMWARE FRONT

Ransomware and extortion attacks never seem to subside, and they give asset owners and operators plenty to consider when it comes to risk assessments; a recent Claroty survey, for example, said 80% of critical infrastructure has been attacked by ransomware, and 60% have paid ransoms. While the 2H 2021 lacked a dramatic major incident, the first six months of the year demonstrated to threat actors that critical infrastructure and OT assets run alongside vulnerable IT technology that can be targeted to impact critical processes and services.

Incidents at Colonial Pipeline, JBS, and NEW Cooperative, just to mention a few, were largely profit-motivated attacks where cybercrime operators researched and understood their victims' willingness to pay hefty ransoms. In each case, attackers demanded millions of dollars in return for restored systems, and Colonial and JBS did reportedly adhere to their attackers' demands.

Critical infrastructure operators, in particular, must now consider whether ransomware attacks are a cover for a far deeper type of attack. As tensions deepened between Russia and Ukraine in January and February, destructive malware attacks were reported against government websites in Ukraine. Using ransomware as a misdirection tactic, Ukrainian systems were instead infected with wiper malware that rendered hard drives on compromised machines useless. These types of misdirection attacks force defenders to spend needless time addressing what they believe to be a ransomware attack only to discover it's a far more impactful intrusion.

In 2022, asset owners and operators should be aware of these types of nation-state tactics, and how kinetic conflicts can also spill online. As conflicts escalate, users should have adequate threat intelligence in order to keep abreast of tactics, techniques, and procedures used to target their infrastructure. Tightening firewall rules, blocking webmail to counter phishing attacks, backing up regularly, storing backup files offline and off-site, and securing OT project files are key strategies to remember as geopolitics enters cyberspace.

ABOUT CLAROTY TEAM82

Claroty's Team82 is an award-winning group of operational technology (OT) researchers, known for its development of proprietary OT-related threat signatures, OT protocol analysis, and the discovery and disclosure of industrial control system (ICS) vulnerabilities. Committed to strengthening OT security and equipped with the industry's most extensive ICS testing lab, Team82 works closely with leading industrial automation vendors to evaluate the security of their products.

To date, Team82 has discovered and disclosed more than **260** ICS vulnerabilities, **110** of which were disclosed during the 2H of 2021.

Recognizing the critical need to understand the ICS risk and vulnerability landscape and how the vulnerabilities discovered by Claroty researchers fit into that picture, Team82 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. These sources encompass the complete breakdown of commercial devices operating in critical infrastructure, manufacturing, healthcare, and other critical industries.

The outputs of this tool expose 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 2021

Team82 discovered and disclosed 110 vulnerabilities in 2H 2021, bringing Claroty's number of disclosures in 2021 to 184. Overall, Team82 has disclosed more than 260 vulnerabilities affecting ICS and IoT devices, and OT protocols.

Team82 prioritizes its ICS research on a number of parameters to provide the greatest benefit and contribution to the ICS domain and security community. Team82 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 in use by Claroty customers

Team82's research examines a variety of vendors and products affecting numerous sectors in the industry. Because of these parameters, Claroty also researches third-party products. The **110** vulnerabilities discovered by Team82 in the 2H of 2021 affect 16 automation and technology vendors. The breakdown of affected vendors and ICS product types is as follows in the two charts below:

1.1. AFFECTED ICS VENDORS

A breakdown of the **16** automation and technology vendors affected by the **110** vulnerabilities discovered and disclosed by Team82 in the 2H 2021

VENDORS

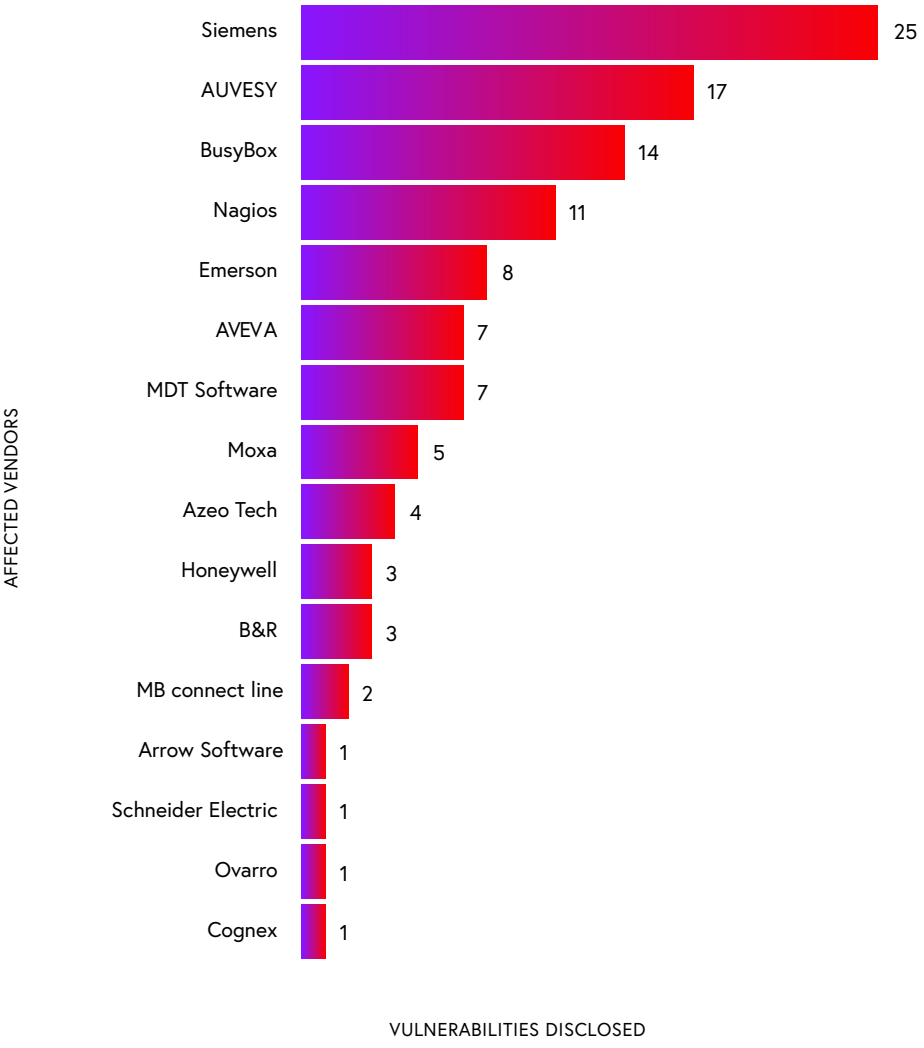


Figure 1.1: Breakdown of vendors affected by Team82 disclosures.

1.2. AFFECTED ICS PRODUCT TYPES

Vulnerabilities disclosed by Team82 were largely found at Level 3 of the Purdue Model: Operations Management.

TARGETED PRODUCT FAMILY

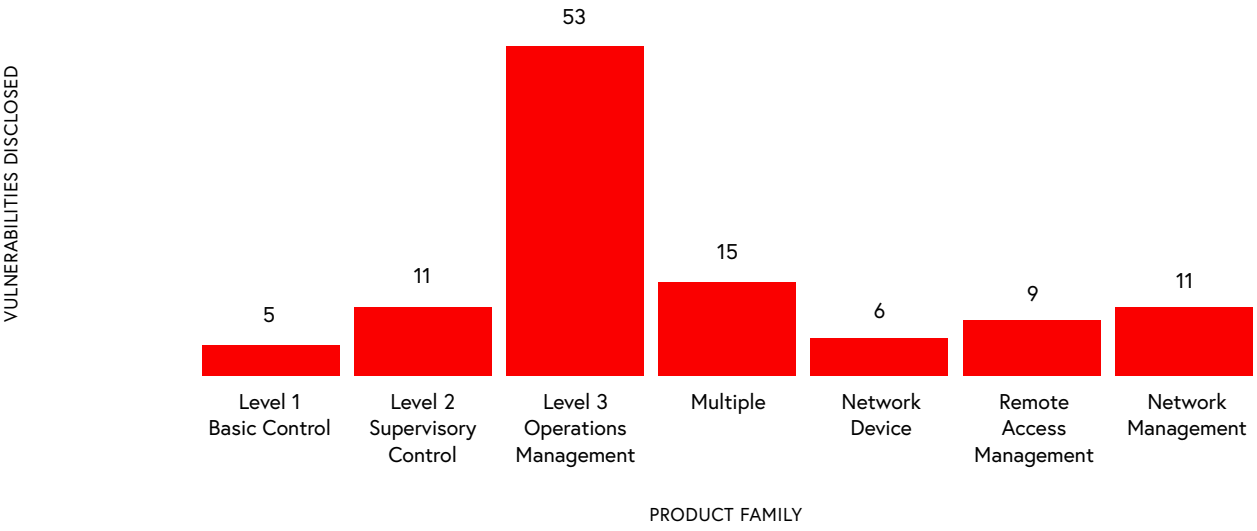


Figure 1.2: Breakdown of vulnerabilities discovered by Team82 by product family type.

PART 2: ASSESSMENT OF ALL ICS VULNERABILITIES DISCLOSED IN 2H 2021

This section provides a statistical analysis and contextual assessment of all ICS vulnerabilities published in 2H 2021.

The data below includes vulnerabilities discovered and disclosed by Team82, in addition to all others publicly disclosed by other researchers, vendors, and third parties during 2H 2021.

2.1. TOTAL COUNT OF ICS VULNERABILITIES

During 2H of 2021, 797 ICS vulnerabilities were published, affecting 82 ICS vendors.

VULNERABILITIES PUBLISHED

797

Total Count of Identified Vulnerabilities

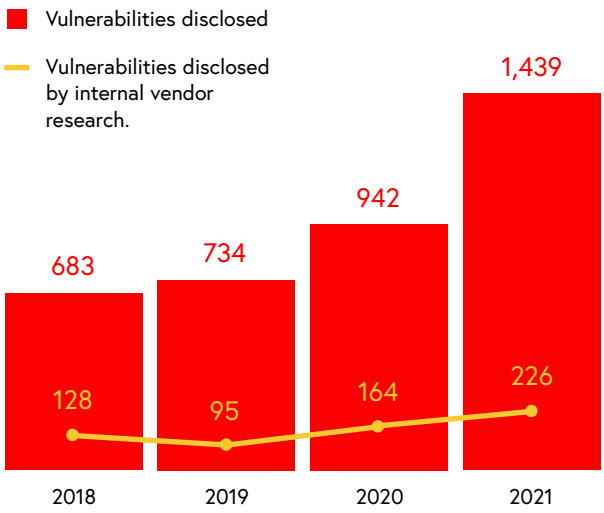
VENDORS AFFECTED

82

Total Count of Affected Vendors

2.2 YEARLY COMPARISON OF ICS VULNERABILITIES

The number of vulnerability disclosures grew significantly over the last four years, demonstrating an increase of awareness and the number of security researchers shifting toward examining OT.



+110% Increase
in vulnerabilities disclosed

+76% Increase
in number of vulnerabilities disclosed by internal vendor research.

Figure 2.2a: Breakdown of vulnerabilities disclosed each year.

2.3 ORIGIN OF VULNERABILITY DISCOVERIES, 2H 2021

In 2H 2021, 80% of vulnerabilities disclosed were discovered by sources external to the affected vendor. The external sources include a number of research organizations, third-party companies, independent researchers, and academics, among others.

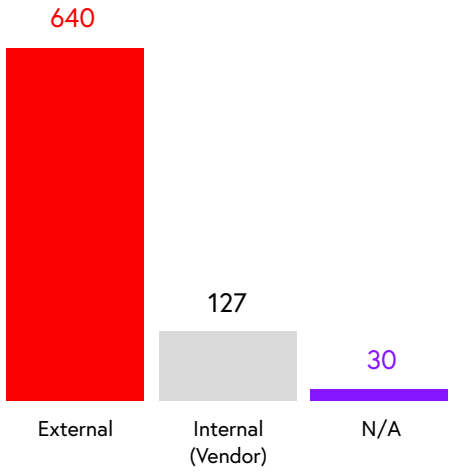


Figure 2.3a: Breakdown of vulnerabilities by origin of discovery.

The chart below breaks down the number of vulnerabilities disclosed by external sources, led by third-party companies. Those sources found **399** vulnerabilities **(50%)** in 2H 2021. Many of these disclosed vulnerabilities were discovered by researchers at cybersecurity companies, indicating a shift in focus to include ICS alongside IT and IoT 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 2021, this accounts for **92** vulnerabilities).

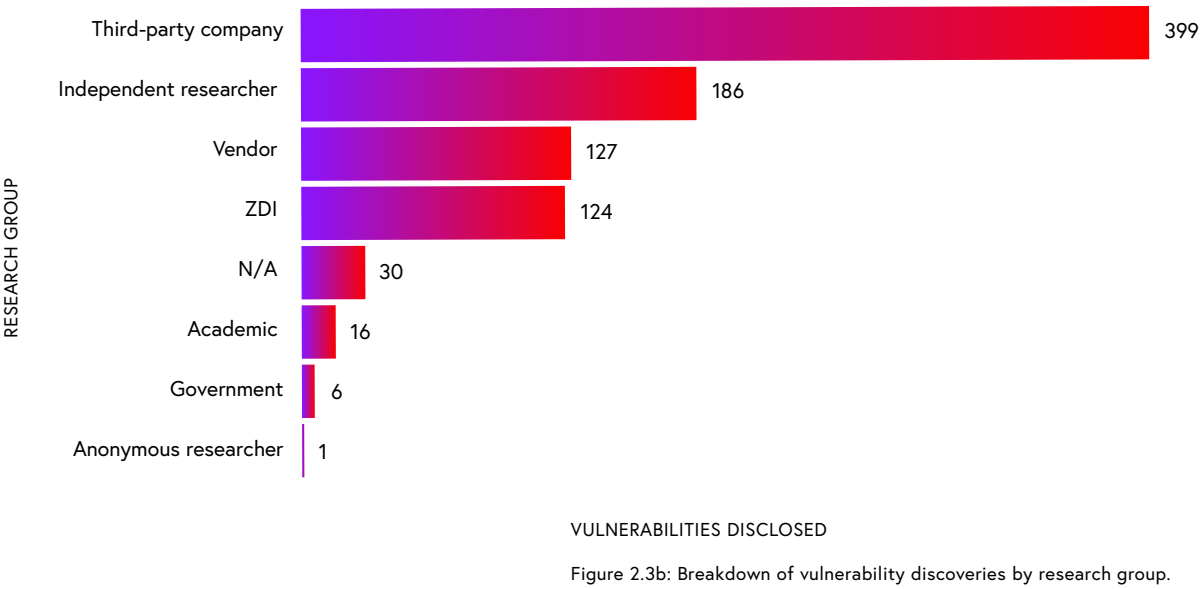


Figure 2.3b: Breakdown of vulnerability discoveries by research group.

Team82 also notes there were **55** new researchers reporting vulnerabilities during 2H 2021; the data in the chart below breaks down those new entrants by type.

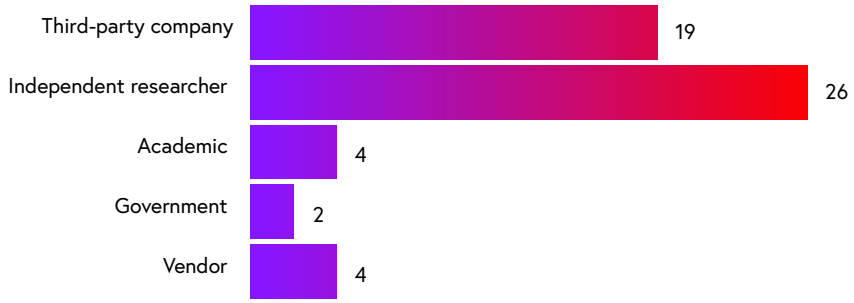
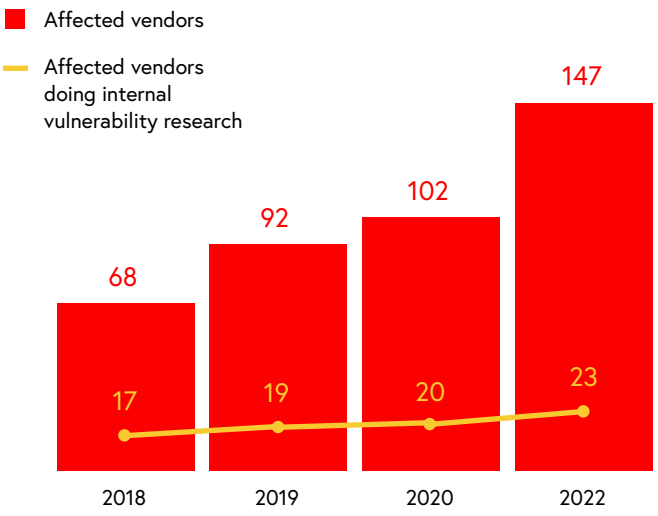


Figure 2.3c: Breakdown of new researchers reporting ICS vulnerabilities.

Team82's data indicates that new researchers focused largely on products from market-leading vendors, such as Siemens, Schneider Electric, and others. Six of the new researchers introduced five newly affected vendors in 2H 2021. The remainder examined previously affected vendors. It should be noted that ICS and SCADA devices and software can be difficult and expensive to acquire, especially for newly active researchers. This is also likely a contributing factor to the focus on market-leading vendors, whose products are more readily available.

2.4 AFFECTED ICS VENDORS

Team82 has compiled trending data across our four biannual reports showing an increase in the number of vendors affected by vulnerabilities in 2021.



+116% Increase in affected vendors

+35% Increase in affected vendors doing internal vulnerability research

Figure 2.4a: Breakdown of affected vendors each year.

While there is a noteworthy bump in the number of vendors affected by vulnerabilities in 2021, it's important to understand some of the factors behind those numbers. Vulnerability research within OT and ICS is still a maturing discipline, and Team82's dataset also shows an upward trend in the number of vendors doing internal vulnerability research and disclosing vulnerabilities.

Large vendors such as Siemens AG, Schneider Electric, and Rockwell Automation have mature, established product security teams whose task is to deliver secure, reliable products to customers. Team82 has forged research partnerships with these leading automation vendors, and with many others who are formulating and nurturing their own internal security and response teams. The end result is a largely more secure ecosystem.

Also, a significant number of disclosed vulnerabilities for any one vendor is not a reflection of its ability to scrutinize products for security issues. In fact, the opposite is likely true to where these affected vendors are allocating ample dedicated resources to product security and are likely to discover a greater number of vulnerabilities. The age, catalog, and install base of each vendor also tend to influence the number of disclosed vulnerabilities affecting products.

In the current Team82 dataset, Siemens was the vendor with the most reported vulnerabilities at **251** (many of which were disclosed as part of internal research conducted by the Siemens ProductCERT team) followed by Schneider Electric, Advantech, Delta Electronics, and Mitsubishi.

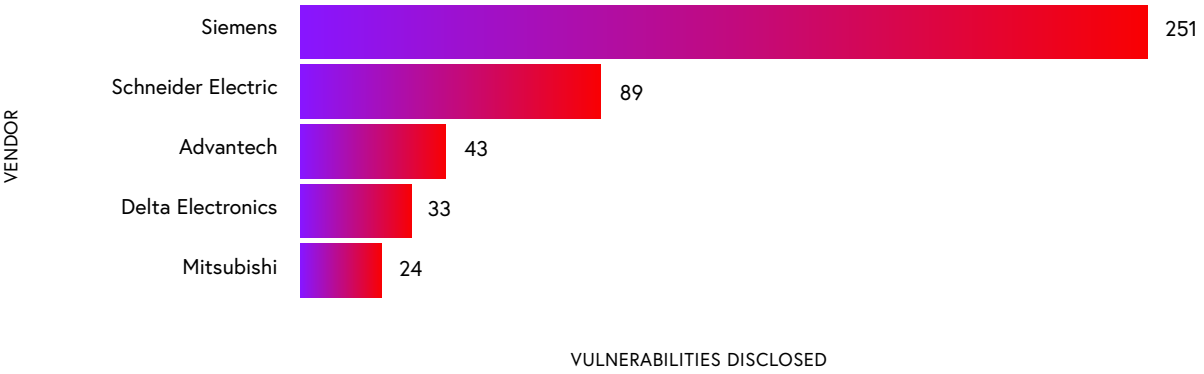


Figure 2.4a: Breakdown of affected vendors each year.

2.5 VENDORS WITH FIRST-TIME VULNERABILITY DISCLOSURES IN 2H 2021

21 vendors whose products had not been previously affected by ICS vulnerabilities were impacted by at least one ICS vulnerability disclosed in 2H 2021.

8 of these vendors specialize in automation, **4** in healthcare, and **4** in manufacturing.

Vendors	Primary Industry
AzeoTech	Automation
AUVESY	Automation
Arrow Software	Automation
mySCADA	Automation
MDT Software	Automation
Bachmann Electronic	Automation (Renewable Energy)
Cognex	Automation, Manufacturing (Machine Vision)
FANUC	Automation, Manufacturing (Robotics)
Boston Scientific	Healthcare (Medical Equipment & Devices)
Swisslog Healthcare	Healthcare (Pharma supply chain)
Fresenius Kabi	Healthcare (Pharma, Biotech)

Vendors (continued)	Primary Industry
Ypsomed	Healthcare (Pharma, Biotech)
Helmholz	Industrial Communication
InHand Networks	Industrial IoT
Annke	IoT (home & business security)
HCC Embedded	IoT (security)
BusyBox	IT Technology
Nagios	IT Technology
Uffizio	IT Technology (GPS Tracking)
Trane	Manufacturing
Xylem Inc.	Manufacturing (Water Technology)

2.6 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. In 2H 2021, the majority of vulnerabilities affect software components, and given the comparative ease in patching software over firmware, defenders have the ability to prioritize patching within their environments.

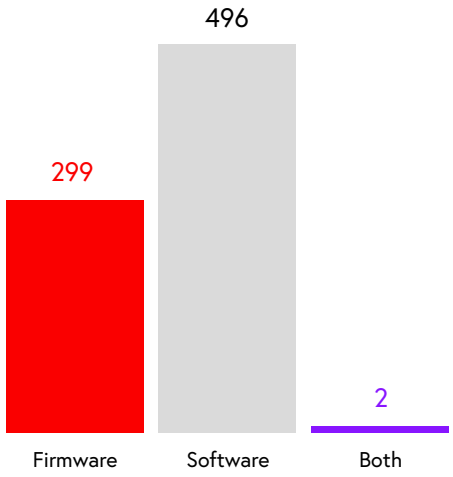


Figure 2.5a: Breakdown of vulnerabilities found in software and firmware.

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 as 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 an HMI, or an ethernet module connected to a pump. The following graph showcases the families of products affected by these vulnerabilities, and the categories are as seen below:

AFFECTED PRODUCT FAMILIES

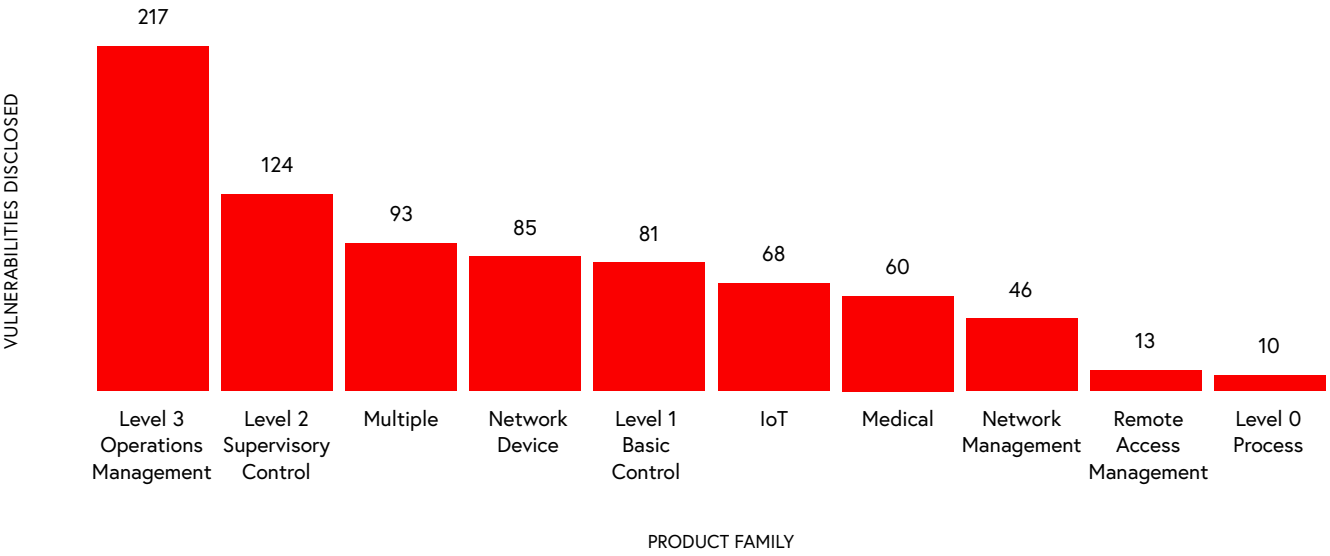


Figure 2.5b: Breakdown of affected product families.

Since **27%** of vulnerabilities affect the Operations Management (Level 3) level of the Purdue Model, below, this explains why we saw many of the vulnerabilities affect software components. In addition, about **25%** 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, making them an attractive target.

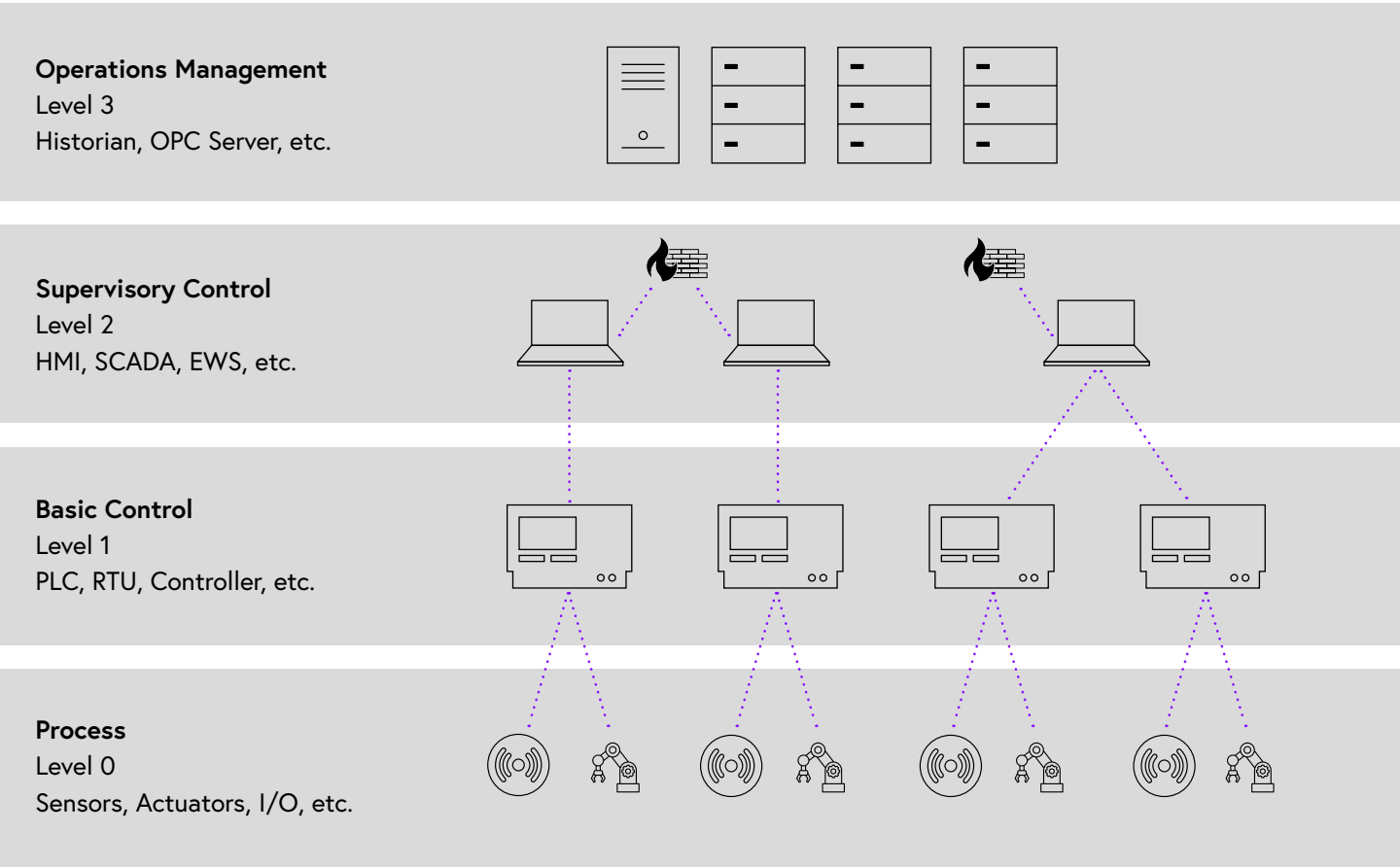


Figure 2.5c: The Purdue Model for industrial control systems.

We want to note the Multiple category: This category mostly contains third-party component vulnerabilities, which often come in bundles of multiple vulnerabilities in each disclosure. They often affect many vendors and products across the industry. It emphasizes that protections and mitigations against third-party vulnerabilities, starting with visibility and risk assessments, are an integral part of OT network security.

When looking into each category, you can divide the vulnerable component affecting them into firmware, software, or both. Most of the Operations Management (Level 3) and 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 because of its links to the Basic Control level.

FIRMWARE/SOFTWARE DIVISION IN PRODUCT FAMILY

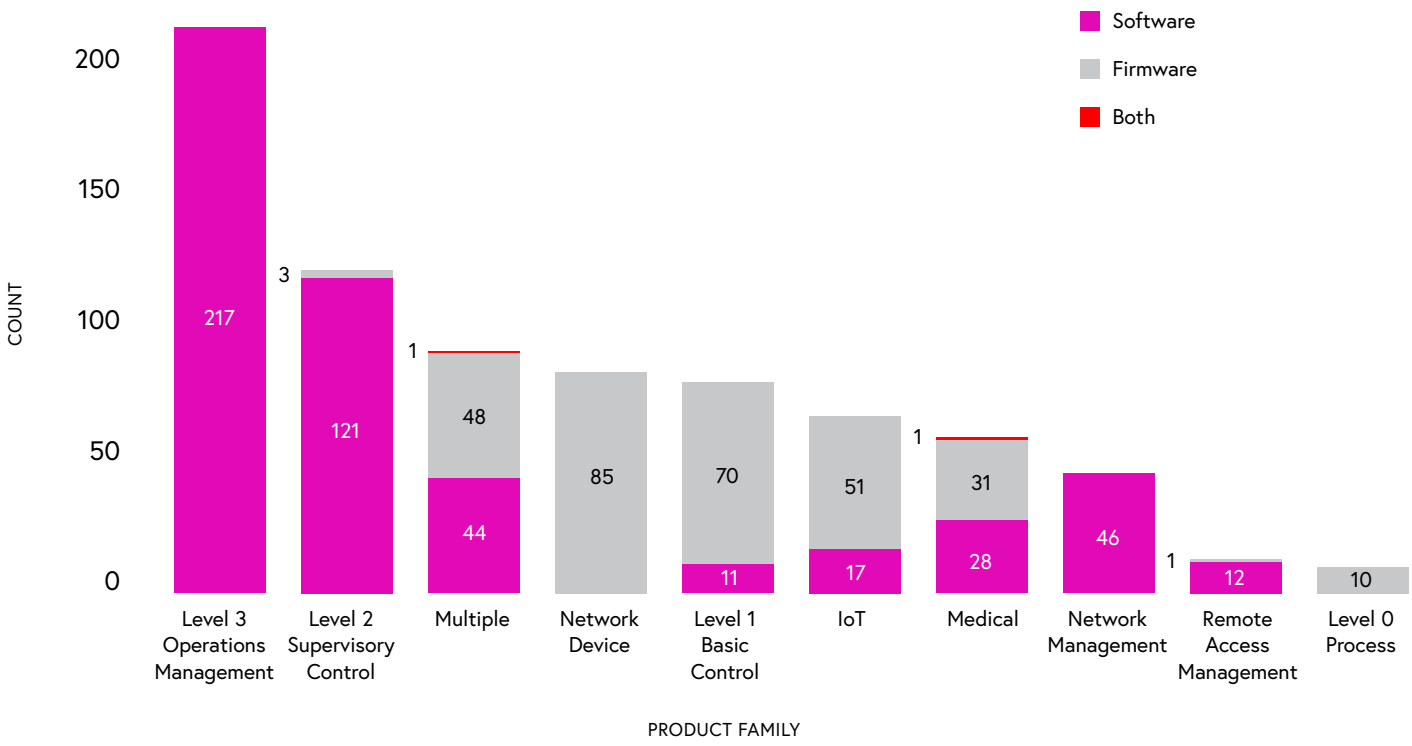


Figure 2.5d: Breakdown of firmware and software vulnerabilities by product family.

PART 3: MITIGATIONS AND REMEDIATIONS

3.1 MITIGATIONS

Mitigations are often the only remediation option open to defenders given the software and firmware patching challenges we've described. Yet despite defenders' dependence on mitigations, vendor advisories or alerts from industry groups such as ICS-CERT sometimes come up short with their defense-in-depth recommendations.

Actionable recommendations such as blocking specific ports or updating outdated protocols are important, but it should be noted that foundational practices must be in place before those recommendations are effective.

Team82's data around the top mitigation steps bears this out, below. For example, network segmentation is the top step, and should be a top consideration for defenders ahead of other options on our list, including ransomware awareness (phishing mitigations), traffic restriction, user- and role-based access policies, and the principle of least privilege.

TOP MITIGATION STEPS

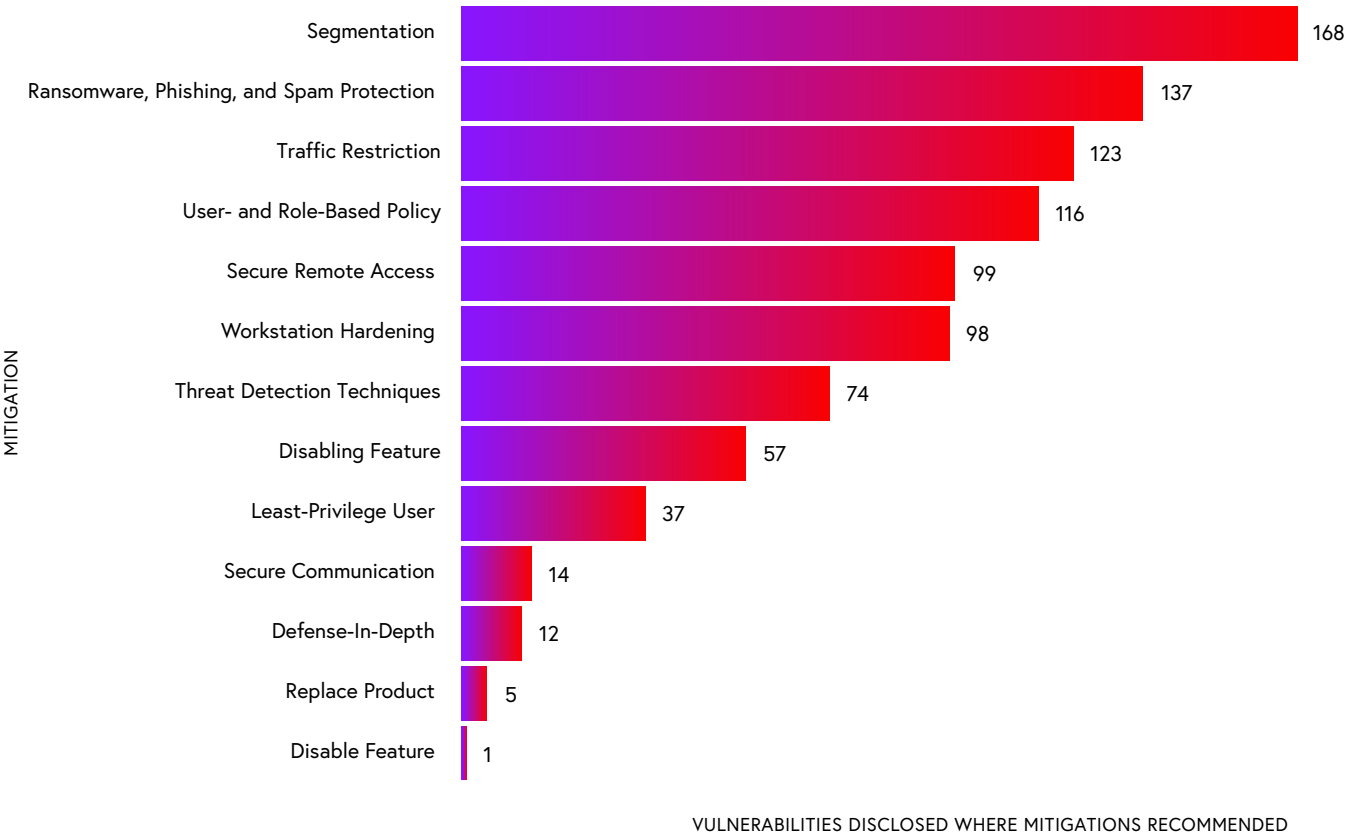


Figure 3.1a: Breakdown of top mitigation steps.

Network segmentation is an important control as air-gaps become a relic of the past, perimeters erode, and enterprises move data, applications, infrastructure, and services to the cloud. Segmentation involves virtual zoning that allows for zone-specific policies tailored to engineering and other process-oriented functions. The ability to inspect traffic and OT-specific protocols is also crucial to defend against anomalous behaviors.

Ransomware, phishing, and spam protection was right behind segmentation as a top mitigation step. Ransomware attacks against IT systems, as demonstrated against NEW Cooperative, Colonial Pipeline, and JBS Foods, must be taken into consideration because they can cross over to systems that manage OT, or force the shutdown of critical processes and services. Maintaining and storing backups offline will enable quicker data restoration when needed and help resume operations. Finally, raising awareness among employees against social engineering and phishing techniques is vital because, as we mentioned earlier, many vulnerabilities exploited via local attack vectors are dependent on user interaction.

3.2 REMEDIATIONS

Vulnerability remediation takes three forms: full remediation, where all affected products have a fix, partial remediation, where not all affected versions of products have a fix, and no remediation whatsoever.

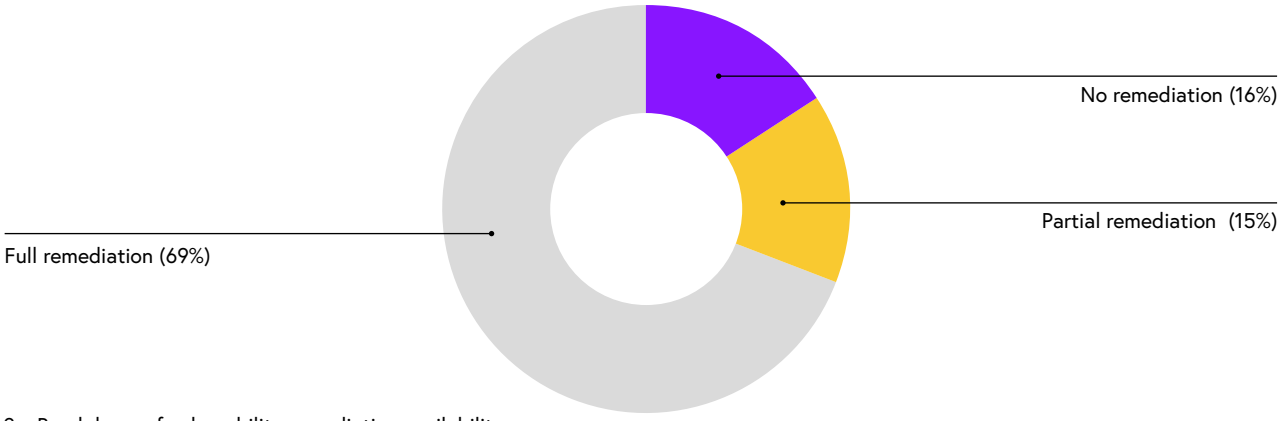
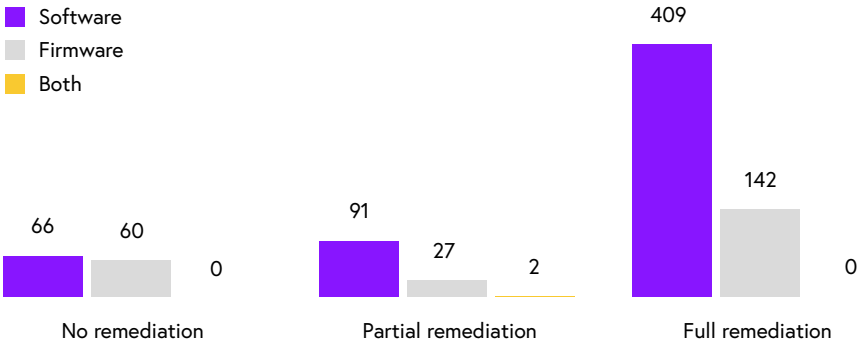


Figure 3.2a: Breakdown of vulnerability remediation availability.

Breaking down vulnerability remediation by software and firmware can help security practitioners create a strategic remediation and mitigation plan.

REMEDIATION BY FIRMWARE/SOFTWARE



74% **of fully remediated vulnerabilities** are software-based. Given the comparative ease in patching software over firmware, defenders have the ability to prioritize patching within their environments.

62% **of partially or unremediated vulnerabilities** when exploited, could result in remote code execution or denial-of-service.

Figure 3.2b: Breakdown of vulnerability remediation availability by firmware/software.

When looking into the products for which there is a software fix (partial or full), the majority are in Level 3: Operations Management, followed by Level 2: Supervisory Control and Network Management.

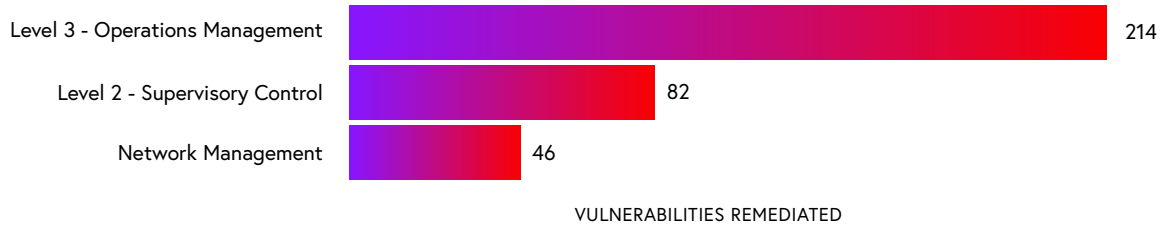


Figure 3.2c: Breakdown of top three software remediations availability by product family.

For firmware, in addition to the inability to update over time, there is also the issue of having fewer remediation solutions available. When firmware remediations exist (partial or full), Team82's data shows they are largely for network devices, followed by Basic Control (Level 1) and IoT. This demonstrates that even in firmware, some prioritization of updates could happen because updating a network device such as a switch is easier and likelier than upgrading a PLC or RTU.

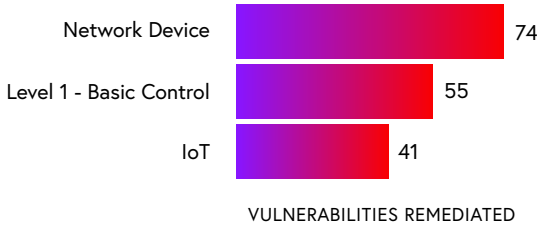


Figure 3.2d: Breakdown of top three firmware remediations availability by product family.

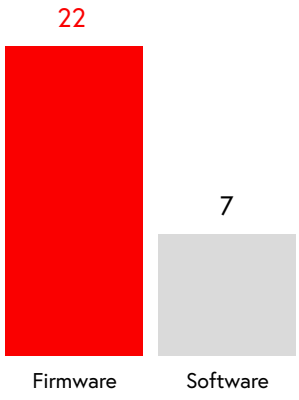
3.3 END-OF-LIFE PRODUCTS

29 vulnerabilities affect **end-of-life** products for which there is no remediation planned because the vendor no longer supports them.

59% **of vulnerabilities affecting end-of-life** products are exploitable remotely via a network attack vector

48% **of vulnerabilities affecting end-of-life** products are found in Level 1 - Basic Control devices such as: PLCs, RTUs etc.

59% **of vulnerabilities affecting end-of-life** products when successfully exploited could lead to code execution or denial-of-service



Other affected end-of-life products include Supervisory Control devices (Level 2), followed by medical and network devices.

When talking about end-of-life products, the only solution is to mitigate (when possible) until replacement. Software updates and patching are easier than firmware updates; firmware updates, however, could take months or years to be developed and distributed. That along with having fewer remediation solutions leads to the understanding that defenders mostly depend on mitigations and are exposed longer to active exploitation.

Vendors and CISOs must track this type of technical debt. Vulnerabilities in unsupported products conflict with the long shelf life of ICS products and may rapidly accumulate. The same goes for supported products that may be running in environments where updates are challenging, in particular where downtime is unacceptable. Unpatched remote code execution and denial-of-service vulnerabilities amplify risk, often to unacceptable levels.

PART 4: CVSS INFORMATION

The Common Vulnerability Scoring System's (CVSS) Base Metrics group represents the characteristics of a vulnerability that are constant over time and user environments, and includes two sets of metrics: exploitability and impact.

4.1 EXPLOITABILITY METRICS

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

As you can see in the following graph, **63%** of vulnerabilities may be exploited through a network attack vector and are remotely exploitable. This emphasizes the importance of protecting remote access connections and internet-facing OT devices.

As for vulnerabilities with a local attack vector **(31%)**, 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. Indeed, attacks exploiting such techniques are on the rise, and employees should adhere to security measures detailed in the recommendations section.

ATTACK VECTOR DISTRIBUTION

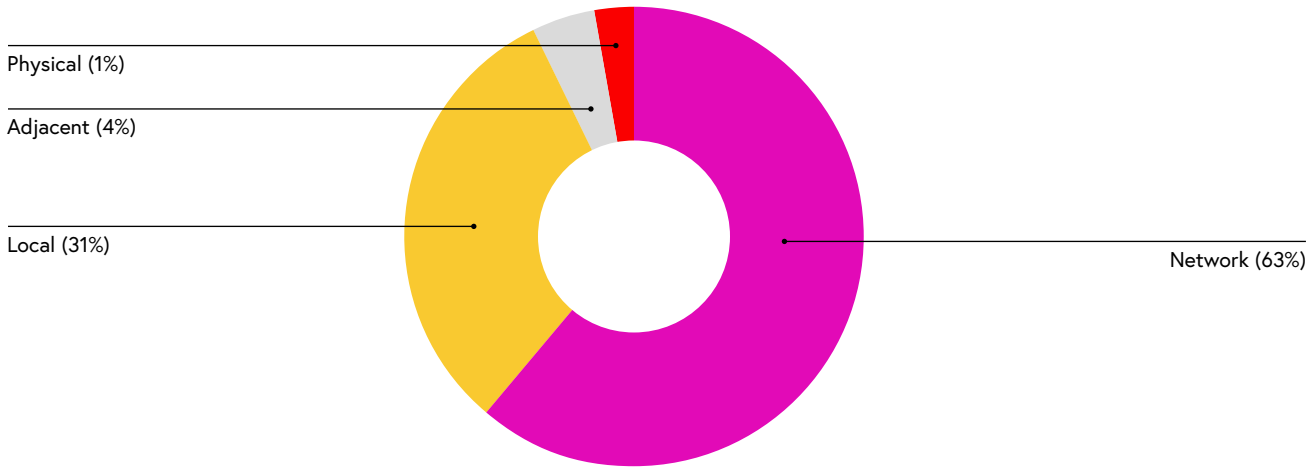
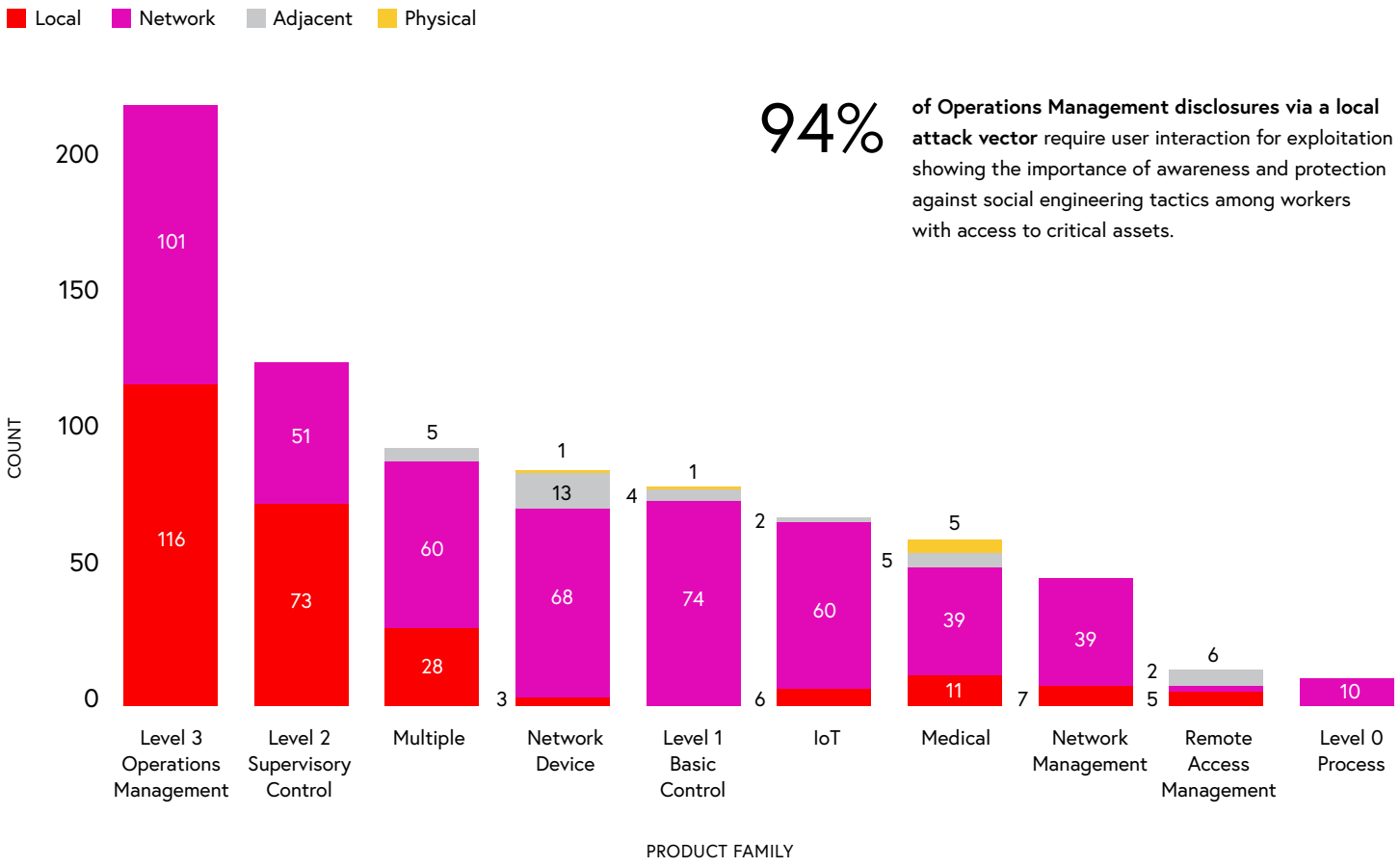


Figure 4.1a: Attack vectors associated with ICS vulnerabilities

ATTACK VECTOR PER PRODUCT FAMILY

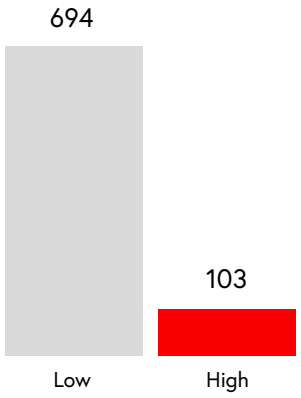


94% **of Operations Management disclosures via a local attack vector** require user interaction for exploitation showing the importance of awareness and protection against social engineering tactics among workers with access to critical assets.

Figure 4.1b: 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.



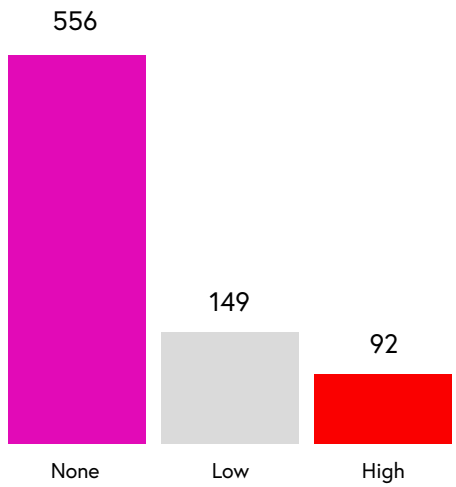
87% **of vulnerabilities are of low complexity** meaning these vulnerabilities don't require special conditions and an attacker can expect repeatable success every time.

Figure 4.1c: Attack complexity according to CVSS scoring.

4.2 PRIVILEGES REQUIRED

This metric represents the level of privileges an attacker must have before successfully exploiting the vulnerability.

CVSS PRIVILEGES REQUIRED



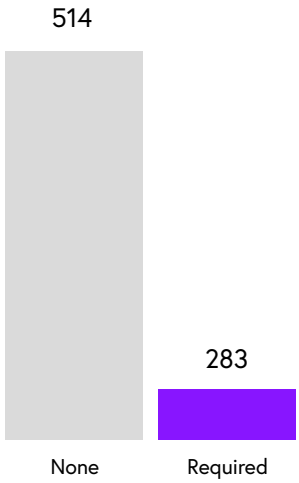
70% **of vulnerabilities require no privilege** meaning the attacker is unauthorized prior to attack and does not require access to the target's settings or files.

Figure 4.2a: Privileges required to exploit vulnerabilities.

USER INTERACTION

This metric represents the dependency of the attacker on the participation of a separate user or user-initiated process in order to exploit the vulnerability.

CVSS USER INTERACTION



64% **of vulnerabilities require no user interaction,** meaning the attacker does not depend on the participation of a seperate user or user-initiated process in order to exploit the vulnerability.

Figure 4.2b: User interaction required by exploit vulnerabilities.

4.3 IMPACT METRICS

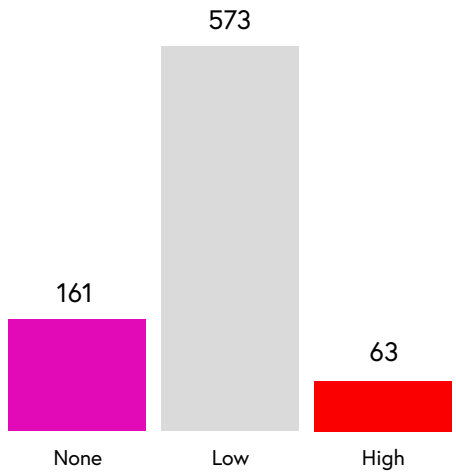
These metrics represent the direct consequences of a successful exploitation of each vulnerability. The CVSS system measures impact according to the CIA triad (confidentiality, integrity, and availability). Though technically relevant to any type of network, the CIA triad does not encompass what are arguably the two most important risk variables for OT networks: reliability and safety.

This means that the CVSS score 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.

CVSS CONFIDENTIALITY



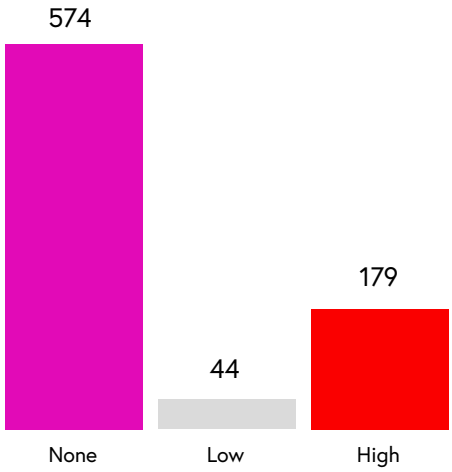
92% **of vulnerabilities have low or no impact on confidentiality** demonstrating that while confidentiality is important in IT security, it acts as a far less significant risk variable in OT networks.

Figure 4.3a: Impact on confidentiality.

INTEGRITY

This metric represents the impact on the integrity of information as a result of successful exploitation of a vulnerability.

CVSS INTEGRITY



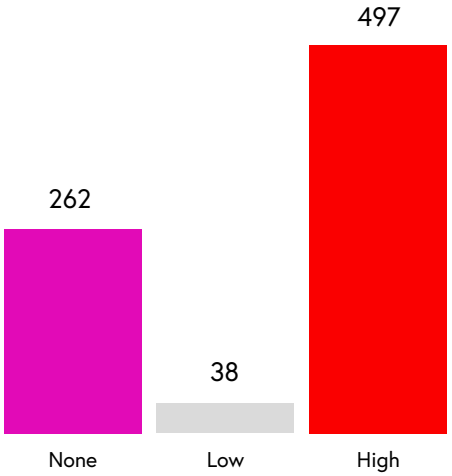
72% **of vulnerabilities have no impact on integrity** Showing that while integrity of information is important in IT security, it is a lesser risk variable in OT networks.

Figure 4.3b: Impact on integrity.

AVAILABILITY

This metric represents the impact to the availability of the impacted component as a result of successful exploitation of a vulnerability.

CVSS AVAILABILITY



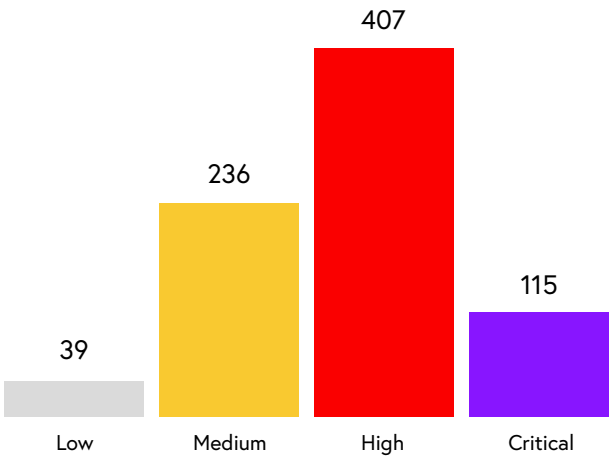
62% **of vulnerabilities have a high impact on availability,** meaning there is a total loss of availability, resulting in denial of access to resources. Alternatively, the loss of availability may be partial but significant–for example, denying the ability to create new connections.

Figure 4.3c: Impact on availability.

4.5 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.

CVSS CATEGORY DIVISION



65% **of vulnerabilities are classified as high or critical**, reflecting the broader tendency among ICS security reseachers to focus on identifying vulnerabilities with the greatest potential impact in order to maximize harm reduction

Figure 4.5a: Breakdown of CVSS scores by criticality.

The CVSS category division 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.

PART 5: EXPLOITED CWEs

The top five most prevalent Common Weaknesses and Enumerations (CWEs) from Team82's dataset are also prominent on MITRE Corp.'s 2021 CWE Top 25 Most Dangerous Software Errors list. These vulnerabilities can be relatively simple to exploit and enable adversaries to inflict serious damage.

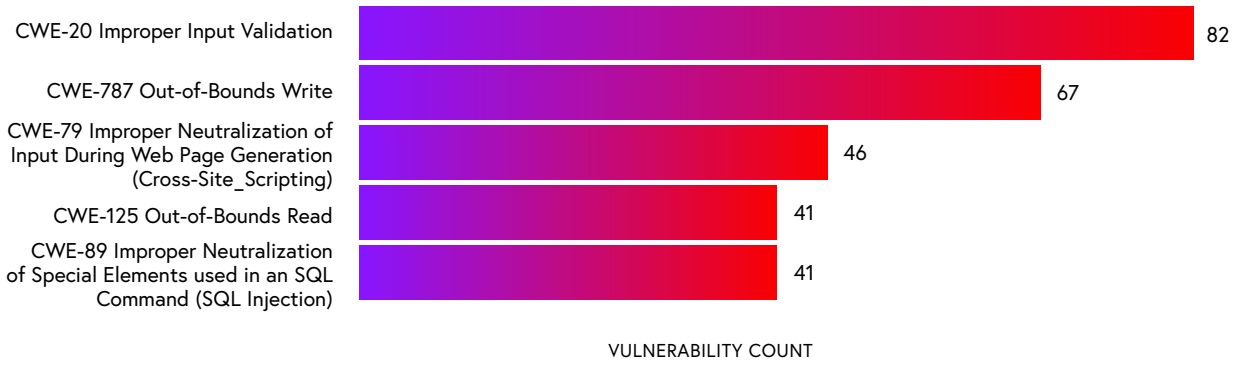


Figure 5a: Breakdown of top five most prevalent CWEs.

CWEs are a category system for software vulnerabilities, a foundation for determining the severity of CVSS scores, and also serve to further emphasize the need to lock down software development practices and implement security measures early on.

Simple coding errors such as input validation, buffer-related memory vulnerabilities, and SQL injection, have long been cautioned against. Yet they continue to plague software development, and this is also reflected in Team82's dataset. One silver lining is that the percentages of all of these CWEs—minus CWE-20—manifested in fewer vulnerabilities during 2H 2021 than the first half of last year. Improper input validation vulnerabilities were the outlier, showing up in 10% of vulnerabilities, up from 4% in 1H 2021.

CWE-787 and CWE-125, out-of-bounds read and write vulnerabilities are Nos. 1 and 3 respectively on MITRE's Top 25 list. They enable a range of outcomes from data corruption and code execution, to denial-of-service attacks.

CWE-79 and CWE-20 are input and neutralization vulnerabilities, and are Nos. 2 and 4 on the MITRE list. Both allow attackers to control flow alterations, modify memory, read application data, bypass protection mechanisms, execute code, or crash devices and processes.

CWE-89 is No. 6 on MITRE's list. It is a failure to neutralize special elements that could be used to modify a SQL command, and result in the attacker being able to read and modify application data and bypass protection mechanisms.

POTENTIAL IMPACTS OF ICS VULNERABILITIES BASED ON CWE

The chart below depicts prevalent potential impacts of ICS vulnerabilities published during 2H 2021 based on CWE. This also reflects 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: causing denial-of-service conditions, bypassing protection mechanisms, and allowing an adversary to read application data, or modify memory.

VULNERABILITY COUNT BY IMPACT

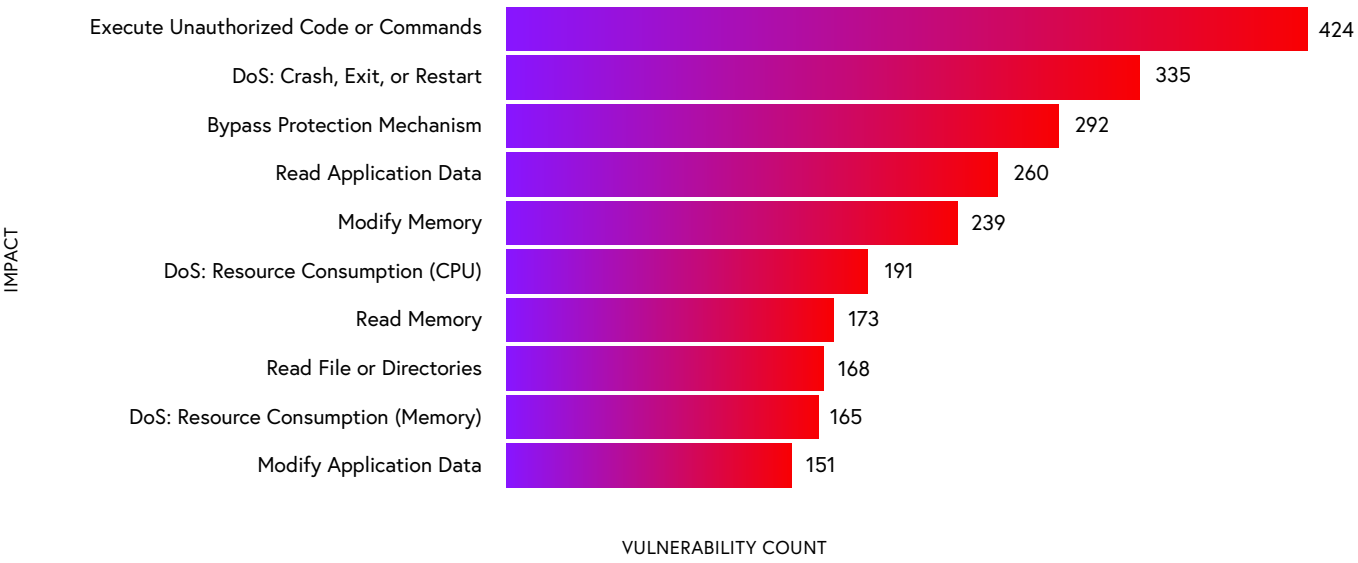


Figure 5a: Breakdown of the number of vulnerabilities by CWE impact.

Among disclosures that target Basic Control devices (Level 1), we found that:

53% may lead to code execution

51% may lead to denial of service

Figure 5b: Impact on Level 1 - Basic Control devices.

Security researchers—and attackers—covet remote code execution vulnerabilities in devices such as PLCs and RTUs. Defending these devices, which are difficult to patch or update, from network-based attacks (91% of these vulnerabilities are exploitable remotely) requires third-party security protection.

PART 6: KEY EVENTS RELEVANT TO THE 2H 2021 ICS RISK & VULNERABILITY LANDSCAPE

Team82 assesses that the following events and trends likely helped shape the ICS risk and vulnerability landscape to a degree during the 2H 2021.

TARDIGRADE BIOMANUFACTURING MALWARE ATTACKS

Polymorphic malware attacks, nicknamed Tardigrade, spread among biomanufacturing companies in November, according to the Bioeconomy Information Sharing and Analysis Center (BIO-ISAC). The attacks were aimed at stealing intellectual property and private research.

Tardigrade's code changed depending on its environment to avoid detection. It stood out from other polymorphic malware because of its ability to recompile its loader from memory and not leave a signature, making its detection even more complicated.

The malware was delivered via numerous vectors, including phishing emails, and used a malware loader known as SmokeLoader, or Dofoil, to inject modules onto compromised machines. It also created a backdoor connection that allowed for downloading files and commands from the attacker's server, deploying additional attack modules, and remaining hidden on the network.

Biomanufacturing companies have been an appealing target for espionage because of their proprietary research and even more so since the beginning of COVID-19 because vaccines and treatments are being developed within this sector. Thus, security practitioners in this industry should remain vigilant.

For further information regarding the Tardigrade biomanufacturing malware attacks refer to:
https://claroty.com/2021/11/24/blog-research-what-you-should-know-about-the-tardigrade-biomanufacturing-malware-attacks/

LOG4J VULNERABILITY

A zero-day vulnerability was uncovered in December in the popular open source Java-based Apache logging framework called Log4J. The vulnerability (CVE-2021-44228), known as Log4Shell, could be abused by remote unauthenticated attackers using a specially crafted string to execute code on affected applications and services. According to a list compiled by CISA, there are more than 100 known affected vendors, and more than 20 are ICS vendors.

As patches and updates surfaced, additional vulnerabilities were discovered rendering previous fixes incomplete in certain non-default conditions. Secondary vulnerabilities could have led to DoS conditions, information disclosure and code execution as attackers can craft malicious input data using a JNDI lookup pattern.

These vulnerabilities affect industrial vendors because the logging utility is used in many applications that are deployed in OT networks leading many vendors to publish patches, mitigations, or lists of affected products.

For further information regarding the Log4J vulnerability refer to:
https://claroty.com/2021/12/14/blog-research-what-you-need-to-know-about-the-log4j-zero-day-vulnerability/

NEW COOPERATIVE RANSOMWARE ATTACK

In September, NEW Cooperative, a farmer cooperative with 60 locations operating in Iowa, shut down its operations following a ransomware attack. The attack was allegedly executed by BlackMatter, an offshoot of DarkSide, the ransomware-as-a-service operation responsible for the Colonial Pipeline attack. BlackMatter reportedly demanded a $5.9M ransom and threatened to double it if it was not paid within five days. In addition BlackMatter allegedly stole 1000 GB of data from NEW Cooperative and threatened to leak it.

During a chat session with BlackMatter, NEW Cooperative stated that 40% of grain production runs on its software and 11 million animals' feed schedules rely on them, meaning a shutdown could break the food supply chain quickly.

NEW Cooperative said it proactively took systems offline to contain the attack, echoing a similar strategy employed by Colonial Pipeline and JBS Foods after disruptive ransomware attacks earlier in 2021.

Companies involved in the food supply chain should protect themselves, ensuring that they have complete visibility into all of their systems and processes while making sure to continuously monitor for any threats that could result from a targeted or opportunistic attack. An accurate asset inventory is the first step toward proper vulnerability management to ensure critical systems are up to current patching levels and compensating controls are in place when appropriate.

For further information regarding the NEW Cooperative attack refer to:
https://www.claroty.com/2021/09/21/blog-food-supply-chain-latest-ransomware-target/

PART 7: RECOMMENDATIONS

Team82 recommends these security measures in response to vulnerability trends we're sharing in this report.

NETWORK SEGMENTATION

As air-gapped industrial devices become a thing of the past, and more devices are connected to the internet and managed via the cloud, defense-in-depth measures such as network segmentation must be prioritized. Network administrators are recommended to:

- Segment networks virtually and configured in such a way they can be managed remotely
- Create zone-specific policies that are tailored to engineering and other process-oriented functions.
- Reserve the ability to inspect traffic and OT-specific protocols in order to detect and defend against anomalous behaviors.

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 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 (sensitive information is also used for double 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
- Enforce multi-factor authentication

PROTECT REMOTE ACCESS CONNECTIONS

Remote workforces are the new normal, and as organizations satisfy demand for increased remote connections to corporate resources, they must do so securely. Within OT environments and critical infrastructure, this is critically important as operators and engineers will require secure remote access to industrial assets in order to ensure process availability and safety. Security practitioners are encouraged to do the following:

- Verify VPN versions are patched and up to current versions
- Monitor remote connections, particularly those to OT networks and ICS devices
- Enforce granular user-access permissions and administrative controls

PROTECTING OPERATIONS MANAGEMENT AND SUPERVISORY CONTROL

The majority of ICS and SCADA vulnerabilities disclosed during 2H 2021 affected Level 3: Operations Management (Historian, OPC Server, etc) followed by the Level 2: Supervisory Control (HMIs, SCADA and engineering workstations).

Most of the Operations Management and 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 Operations Management and Supervisory Control levels, because they provide 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 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 to defend against social engineering techniques.

ACKNOWLEDGEMENTS

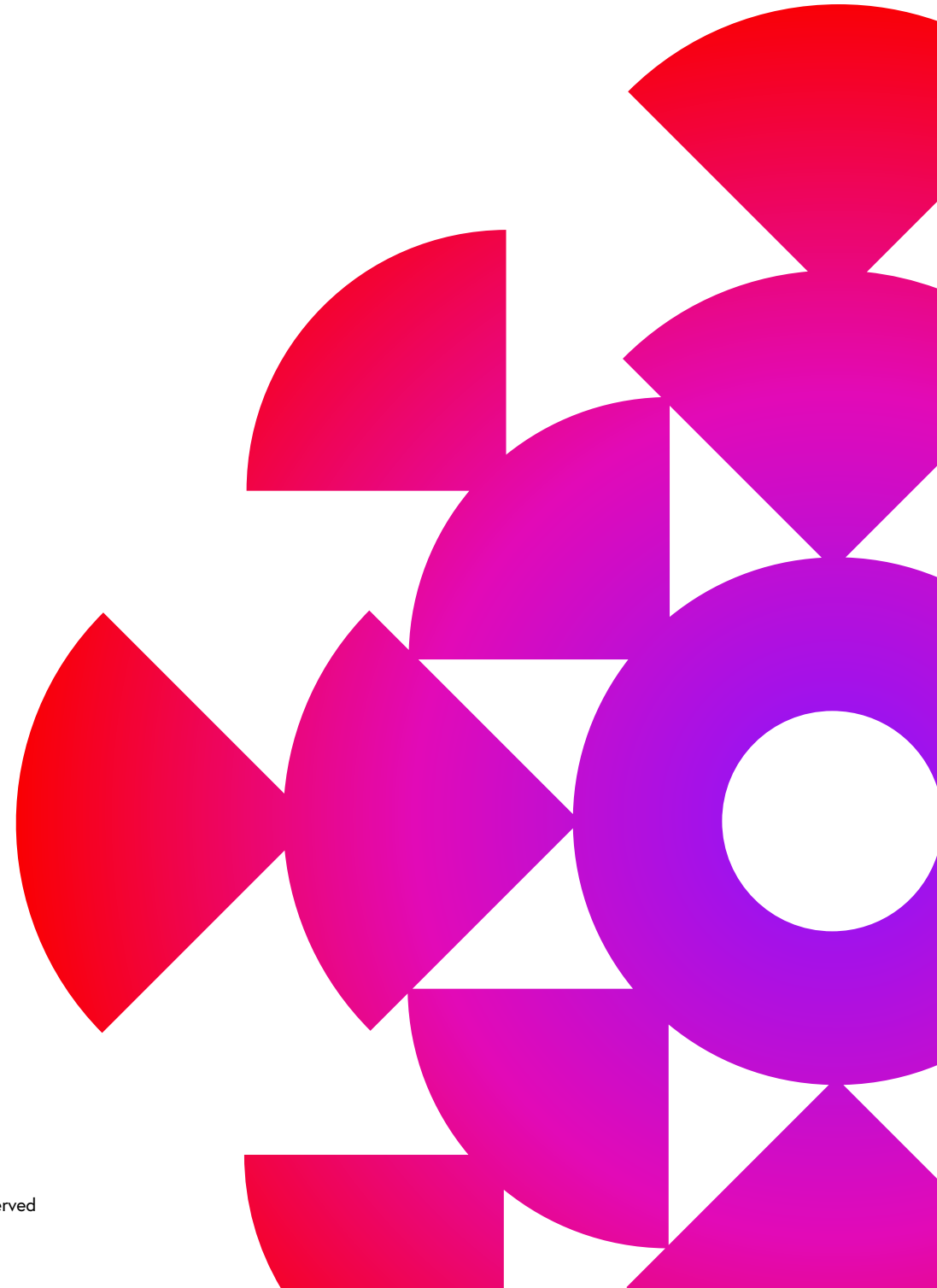
The primary author of this report is Chen Fradkin, security researcher at Claroty.

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 entirety of Team82 for providing exceptional support to various aspects of this report and research efforts that fueled it.

ABOUT CLAROTY

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

To learn more, visit www.claroty.com.



CLAROTY