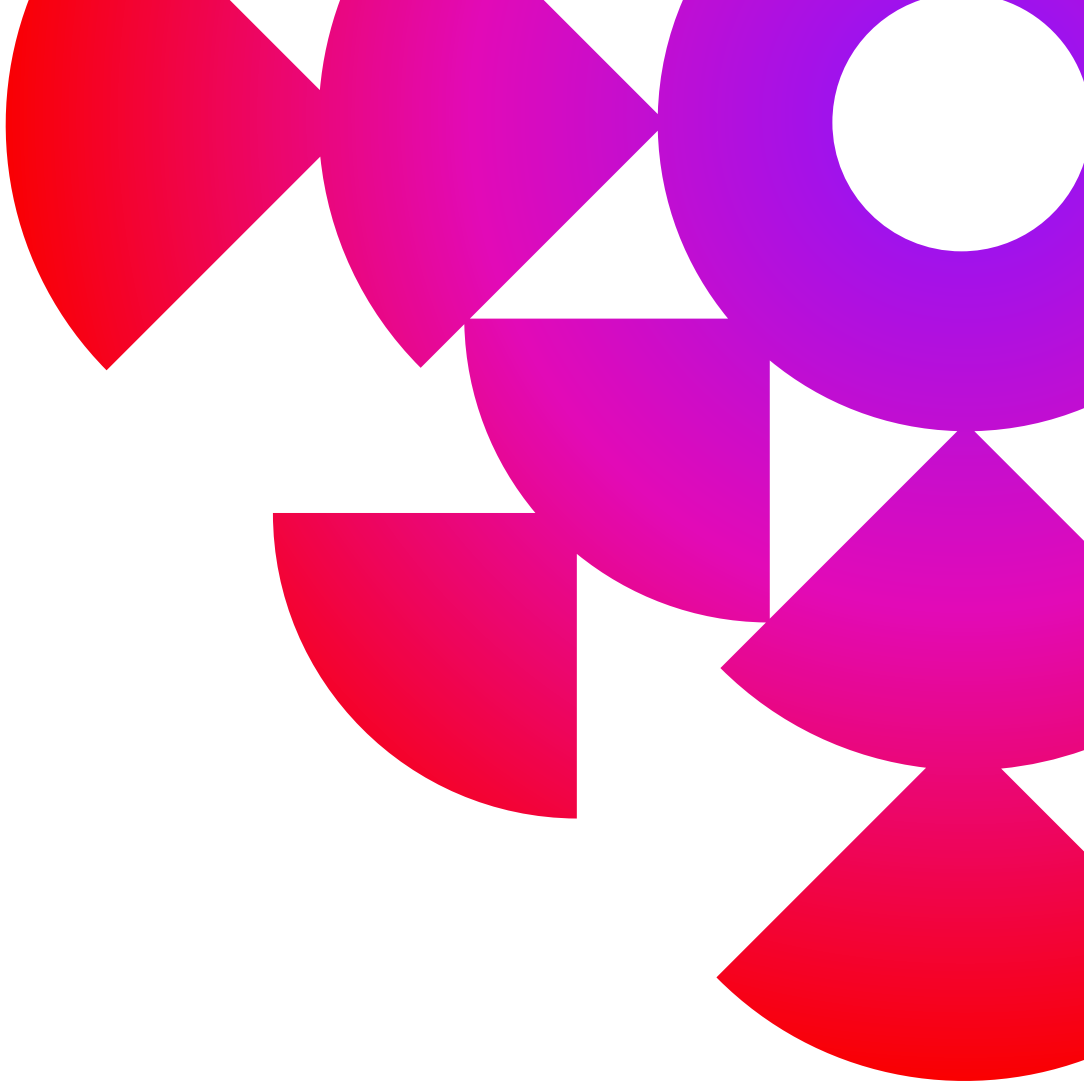


# CLAROTY BIANNUAL ICS RISK & VULNERABILITY REPORT: 1H 2021

By Claroty Team82

CLAROTY

https://t.me/learningnets

# CONTENTS



https://t.me/learningnets

# EXECUTIVE SUMMARY

The first half of 2021 was the biggest test of industrial cybersecurity in history.

Many companies are enjoying the fruits of connecting devices to the internet and converging operational technology (OT) under IT systems management. Yet that momentum has also beaconed out to threat actors, particularly those whose trade is extortion and profit. Assets are exposed online in record numbers, and along with them, all their blemishes: unpatched vulnerabilities, unsecured credentials, weak configurations, and the use of outdated industrial protocols.

In the first six months of the year, all of this conspired to bring us attention-grabbing ransomware attacks against Colonial Pipeline and JBS Foods, an eye-opening intrusion at the water treatment facility in Oldsmar, Fla., and another in the Bay Area. These incidents elevated the security of industrial control systems and OT networks to mainstream conversations.

The U.S. government took notice too, calling out the criticality of securing these systems and networks for the first time in executive orders, a National Security Memorandum, and in sector-specific efforts to improve not only awareness among owners and operators, but to emphasize the overall threat to national security and public safety that attacks against industrial control systems (ICS) and OT can deliver.

Claroty, today, publishes its third Biannual ICS Risk & Vulnerability Report. The report is our research team's (Team82's) effort to define and analyze the vulnerability landscape relevant to leading automation products used across the ICS domain. Team82 delivers a comprehensive look at ICS vulnerabilities publicly disclosed during the first half of the year, including those found by Team82 and those found by affected vendors, independent security researchers, and experts inside other organizations.

The report is an important resource for OT security managers and operators, delivering 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: 1H 2021:

## ICS SECURITY RESEARCH AND DISCLOSURE TRENDS

- During 1H 2021, **637** ICS vulnerabilities were published, affecting products sold by 76 vendors. In our 2H 2020 report, **449** vulnerabilities were disclosed, affecting **59** vendors. **70.93%** of the vulnerabilities are classified as high or critical, about on par with the 2H of 2020.
- Claroty's Team82 disclosed **70** vulnerabilities that were patched or mitigated in the 1H of 2021. Those vulnerabilities affected **20** automation and technology vendors.
- In the 2H of 2020, Team82 disclosed **41** vulnerabilities affecting **14** vendors.
- **80.85%** of vulnerabilities disclosed during 1H 2021 were discovered by sources external to the affected vendor, including a number of research organizations, such as third-party companies, independent researchers, and academics, among others.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

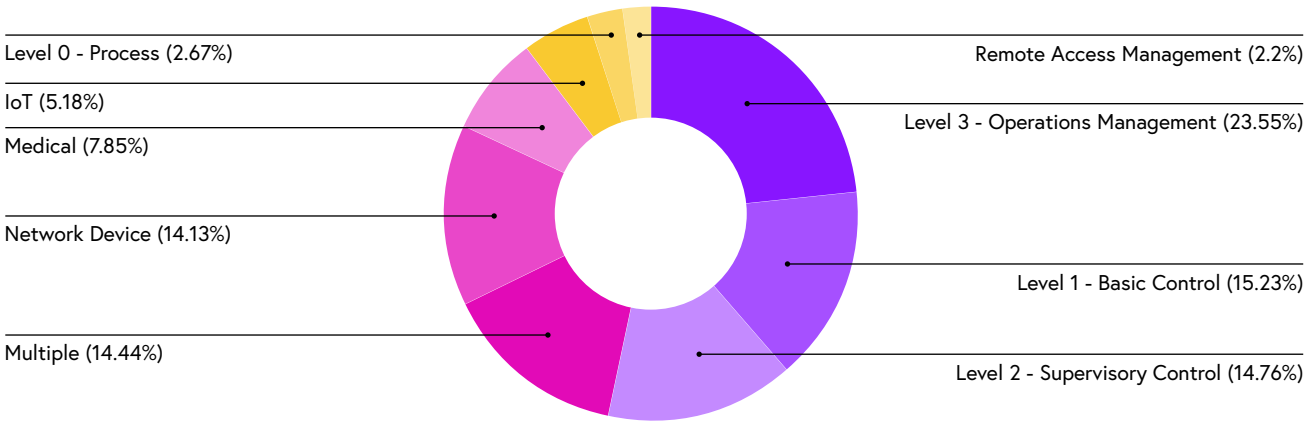
- **42** new researchers disclosed vulnerabilities reported publicly in the 1H 2021. New researchers focused on market-leading automation vendors, but also introduced four newly affected vendors.
- Siemens was the affected vendor with the most reported vulnerabilities, **146**, many of which were disclosed as part of internal research conducted by the Siemens CERT.
- **20** vendors whose products had not been affected by ICS vulnerabilities disclosed in 2020 had at least one disclosure during 1H 2021.

## THREATS AND RISKS FROM ICS VULNERABILITIES

- The largest percentage of vulnerabilities disclosed during 1H 2021 affected Level 3 of the Purdue Model: Operations Management (23.55%), followed by the Level 1: Basic Control (15.23%) and Level 2: Supervisory Control (14.76%).

  Operations Management can be a critical crossover point with converged IT networks. These systems include servers and databases vital to production workflow, or those that collect data that will be fed to higher-level business systems, some of those operate in the cloud. 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




https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

- It's critical that defenders understand the attack vectors threat actors may take to compromise industrial networks. Having proper visibility into potential weak spots helps organizations prioritize patching and other risk management activities. Our data concentrates on two primary attack vectors: remote and local.

  **Remotely Exploitable Vulnerabilities:** Team82's data shows that **61.38%** of security vulnerabilities enable attacks from outside the IT or OT network; that number is down from the 2H of 2020, when **71.49%** were remotely exploitable.

  **Local Attack Vectors:** On the other hand, vulnerabilities exploitable through local attack vectors rose to **31.55%** from **18.93%** in the 2H 2020. For **72.14%** of those vulnerabilities, the attacker relies on user interaction to perform actions required to exploit these vulnerabilities, such as social engineering through spam or phishing. Digging further:

  - In **94.38%** of the Operations Management vulnerabilities via a local attack vector, user interaction would be required for exploitation. This reinforces the need for phishing and spam prevention, as well as awareness techniques that would help stem the tide of ransomware and other potentially devastating attacks.

  - For **39.87%** of local attack vector vulnerabilities, there is no requirement for user interaction and the complexity of exploitation is considered low. An attacker can expect repeatable success every time and does not require privileges to access target settings or files.

- For **65%** of the vulnerabilities, there's a high likelihood of a total loss of availability.

- Updating industrial control systems 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.

  **Mitigations and Remediation:** Team82's data correlates with these trends.

  - **25.59%** of the 637 ICS vulnerabilities disclosed in 1H 2021 have no fix or only a partial remediation.

  - Of the vulnerabilities with no, or partial, remediation, **61.96%** were found in firmware.

  - Of the vulnerabilities with no, or partial, remediation, **55.21%** could result in remote code execution, and **47.85%** could result in denial-of-service conditions when exploited successfully.

  - Of the **74.4%** vulnerabilities with remediation, **59.49%** require software fixes.

  - **6.43%** of the 637 vulnerabilities affect end-of-life products that are no longer supported, meaning the product should be replaced. If a rip-and-replace is not possible, then any recommended mitigations should be applied.

  - **51.22%** of the vulnerabilities affecting end-of-life products were found in firmware.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# TRENDS TO WATCH

Before we take a deeper dive into the numbers from Team82's vulnerability disclosure data for the 1H 2021, it's important to understand three important trends that are likely to drive activity for at least the next six months: OT cloud migration, the relentless extortion and ransomware attacks targeting critical infrastructure and OT, and impending U.S. cyber legislation.

## OT CLOUD MIGRATION

There's an undeniable momentum driving enterprises to bring the cloud to industrial processes. Doing so provides businesses with a number of critical benefits, including:

- Better telemetry and analysis of device performance
- Management of logic and remote device configuration
- Improved diagnostics and troubleshooting
- A centralized view of processes
- Redundancy, critical to business continuity

This is digital transformation personified, and when companies begin to manage OT along with IT from the cloud, that convergence will bring with it many shared risks.

OT, once air-gapped, would now be connected to the cloud and have a much larger attack surface available to attackers. And as the number of organizations bringing the cloud to OT grows, threat actors may see an opportunity to target vulnerabilities suddenly exposed by connectivity at scale. This could be a boon for additional ransomware and extortion-style attacks that impact industrial operations, even tangentially as in the case of Colonial Pipeline and JBS Foods.

Data security, once a lesser risk variable for industrial processes, would also be elevated as a priority, in particular in heavily regulated industries where compliance is unforgiving. Organizations must evaluate not only threats, but risks such as a lack of protocol support for encryption and authentication.

Encryption, for example, may blind some tools from gaining full visibility into network assets. In an air-gapped environment, this can be considered an acceptable risk, but once an asset is exposed online, this is a different scenario. Data should be encrypted in transit as a best practice, and at rest to ensure adequate recovery in the event of an incident. This will be especially evident as companies begin to put services and applications such as Historian databases in the cloud receiving data from Level 1 devices such as PLCs.

Authentication and identity management must also be part of an organization's defense-in-depth plans for OT in the cloud. The COVID-19 pandemic has accelerated remote work, and already, the Oldsmar incident in February demonstrated the risks associated with inadequate controls around access to systems and privilege management.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

**Cloud Explained:** Migrating to cloud-based infrastructure usually means that a part of an organization's infrastructure (IT or OT) is hosted on remote servers hosted by third-party cloud providers, such as Google, Amazon, and Microsoft. The infrastructure includes a cloud-based management platform to support the different users of an organization's services, for example, administrators or engineers. User- and role-based policies must define what functions the users may execute and what privileges they have according to their roles.

There are three types of cloud computing: public, private, and hybrid.

- **Public:** Cloud computing that is shared across multiple organizations and resources are delivered over the internet.
- **Private:** Cloud computing that is exclusive to a single organization. It can be located on-premises or hosted by a third-party provider and maintained on a private network.
- **Hybrid:** Cloud computing that combines public and private clouds. It allows moving data and services between the two environments.

When referring to OT cloud, these concepts remain the same. Operators and administrators, through the management platform, can deploy settings changes, edit configurations, and manage the plant's network.

The migration of OT networks into cloud-based infrastructures requires an internet connection and creates a single controlling point on all sites managed by the cloud-based management console. Now, one simple vulnerability, such as a lack of token in the authentication process, could allow an attacker to take over the cloud-management console that provides access to all managed devices. Vulnerabilities that are commonly a problem in IT security become a challenge to OT security as well.

## RANSOMWARE AND EXTORTION ATTACKS

While we've yet to see ransomware specifically impact Level 1 devices, threat actors have nonetheless found success in impacting industrial operations. The obvious example is Colonial Pipeline, which shut down fuel delivery up and down the U.S. East coast in an abundance of caution after IT systems—not OT—were infected with ransomware.

Attackers have become more insidious in using ransomware, scouting out victims they believe are most likely to pay high ransom demands. While municipal governments, healthcare, and education were once considered target-rich environments for ransomware actors, large manufacturing operations and critical infrastructure are now in the crosshairs.

Another tactic prevalent among threat actor groups intent on profit: advanced intrusions where sensitive business or customer data is stolen, and the threat of publicly leaking that information accompanies the possibility of having critical systems infected with ransomware. Again, actors are targeting high-value organizations likely to meet their demands, and industrial enterprises are beginning to feel the pain. Both Colonial Pipeline and JBS Foods allegedly paid millions in cryptocurrency to threat actors in order to recover encrypted systems.

As more companies connect ICS devices to the internet and converge OT and IT, visibility into network assets is crucial, as is information about software and firmware vulnerabilities that could be exploited by attackers. Flaws in engineering workstations running on Windows-based machines, for example, could allow an attacker to compromise these crossover points between IT and OT networks and modify processes, or more likely, drop ransomware and impede the delivery of critical services that could impact public safety or national security.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

In addition to email-based threats that propagate phishing attacks, defenders need also to focus on secure remote access and on the concentration of vulnerabilities found in virtual private networks and other network-based attack vectors. More than 60 percent of vulnerabilities in Team82's data are remotely exploitable through a network attack vector. This emphasizes the importance of protecting remote access connections and internet-facing ICS devices, and cutting off attackers before they're able to move laterally across networks and domains to steal data and drop malware such as ransomware.

## PENDING U.S. CYBER LEGISLATION

During the 1H of 2021, the attacks at Oldsmar, Colonial Pipeline, and JBS Foods demonstrated the fragility of critical infrastructure and manufacturing as it's exposed to the internet. The attacks showed how attackers could find weaknesses to change chemical levels in public drinking water, or use commodity ransomware to shut down fuel and food delivery systems.

While this malicious activity elevated attacks against OT to the evening news and other mainstream media, it also awakened the U.S. government. A number of government-backed cyber-related activities specifically called out industrial cybersecurity as critical to national security and to the sanctity of the U.S. economy.

President Joe Biden signed in July a National Security Memorandum for critical infrastructure that established the Industrial Control Systems Cybersecurity Initiative, a voluntary effort aimed at private-sector owners and operators to bring their systems in line with current threats. Performance goals are due from the U.S. government by September and it's inevitable that these voluntary initiatives to deploy technology that provides visibility into OT networks and threat detection will become mandatory.

The memorandum followed an executive order signed in May intent on improving threat information sharing between the private and public sectors, modernization of federal cybersecurity standards, hardening of supply-chain security, the establishment of a cybersecurity safety review board, creation of a standard playbook for responding to cyber incidents, improved detection of incidents on federal networks, and better investigative and remediation capabilities.

This followed a 100-day sprint to improve electric grid cybersecurity that also reinforced the theme of better information sharing between private sector owners of utilities and the government. The Biden administration, through the TSA, also reacted strongly to the Colonial Pipeline incident and issued a security directive mandating improvements to the resilience of pipeline networks that includes mandatory incident reporting within 12 hours of detection, regular vulnerability assessments, and protection against ransomware attacks specifically.

As we look forward, drafts of bills floating through Washington include stringent reporting requirements in the wake of incidents. There must be caution and patience that any of these mandates do not introduce additional risk or unrealistic expectations of under-resourced operators of smaller utilities and critical infrastructure operators.

The government must balance its goals of identifying and removing threat actors from networks against harsh oversight of companies that would benefit instead from guidance and funding. It must also understand the realities around vulnerability management for OT, and the challenges associated with patching industrial equipment in high-availability environments, or in updating decades-old devices that weren't meant to be connected to the internet or updated.

This is the dynamic defenders inside critical infrastructure must contend with, and one that the U.S. government must understand in ensuring that mitigations are available to defenders who need them in the absence of immediate patching options, or until full software or firmware updates are available.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# 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. Fiercely 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 **150** ICS vulnerabilities, **70** of which were disclosed during the 1H of 2021. This number exceeds Team82's disclosures during all of 2020. Claroty also had a vulnerability in one of its products disclosed by a third-party research organization; the flaw was privately disclosed, and an advisory with patch and remediation advice was published in June.

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.

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.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# PART 1: ASSESSMENT OF ICS VULNERABILITIES DISCOVERED BY CLAROTY & DISCLOSED IN 1H 2021

Team82 discovered and disclosed 70 vulnerabilities in 1H 2021, exceeding all of Claroty's disclosures in 2020. Overall, Team82 has disclosed more than 150 vulnerabilities affecting ICS devices and OT protocols.

Team82 prioritizes its industrial control system 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 70 vulnerabilities discovered by Team82 in the 1H of 2021 affect 20 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 20 automation and technology vendors affected by the 70 vulnerabilities discovered and disclosed by Team82 in the 1H 2021.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

### VENDORS

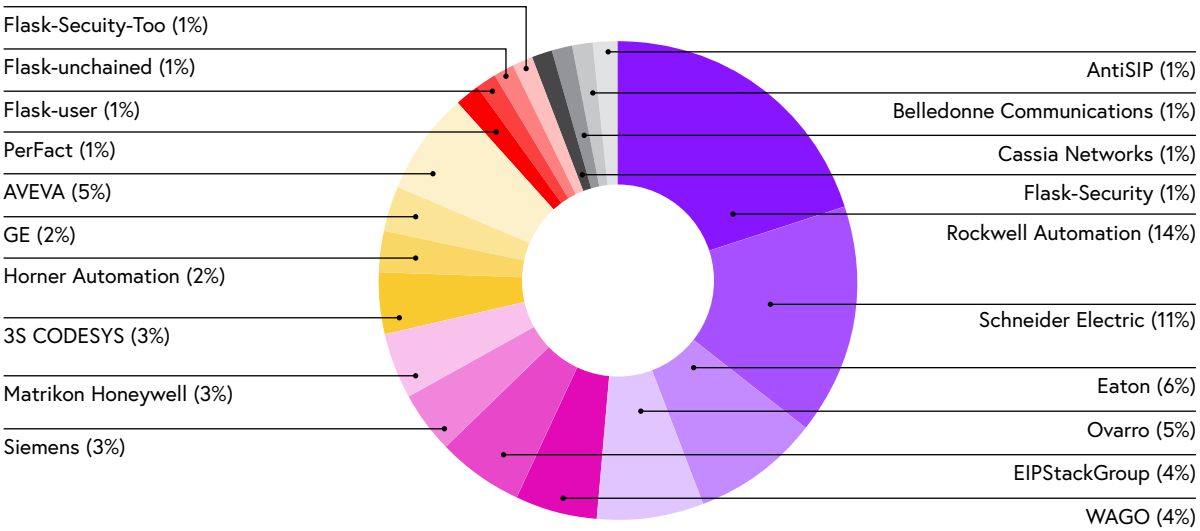



Figure 1.1: Breakdown of vendors affected by Team82 disclosures.

## 1.2. AFFECTED ICS PRODUCT TYPES

Vulnerabilities disclosed by Team82 were largely found at Level 3 of the Purdue Model: Operations Management, and Level 2: Supervisory Control.

### TARGETED PRODUCT FAMILY

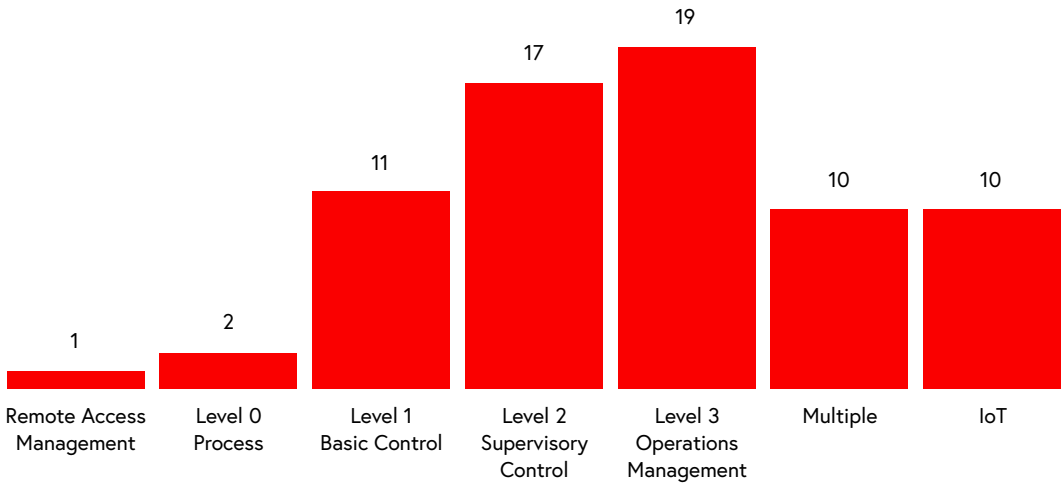



Figure 1.2: Breakdown of vulnerabilities discovered by Team82 by product family type.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# PART 2: ASSESSMENT OF ALL ICS VULNERABILITIES DISCLOSED IN 1H 2021

This section provides a statistical analysis and contextual assessment of all industrial control system vulnerabilities published in 1H 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 the 1H 2021. Team82'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

During 1H of 2021, 637 ICS vulnerabilities were published, affecting 76 ICS vendors:

**VULNERABILITIES PUBLISHED**

637

Total Count of Identified Vulnerabilities

**VENDORS AFFECTED**

76

Total Count of Affected Vendors

## 2.2 ORIGIN OF VULNERABILITY DISCOVERIES, 1H 2021

In 1H 2021, **80.85%** of vulnerabilities disclosed were discovered by sources external to the affected vendor. The external sources include a number of research organizations, including third-party companies, independent researchers, and academics, among others.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## VULNERABILITY RESEARCH ORIGIN

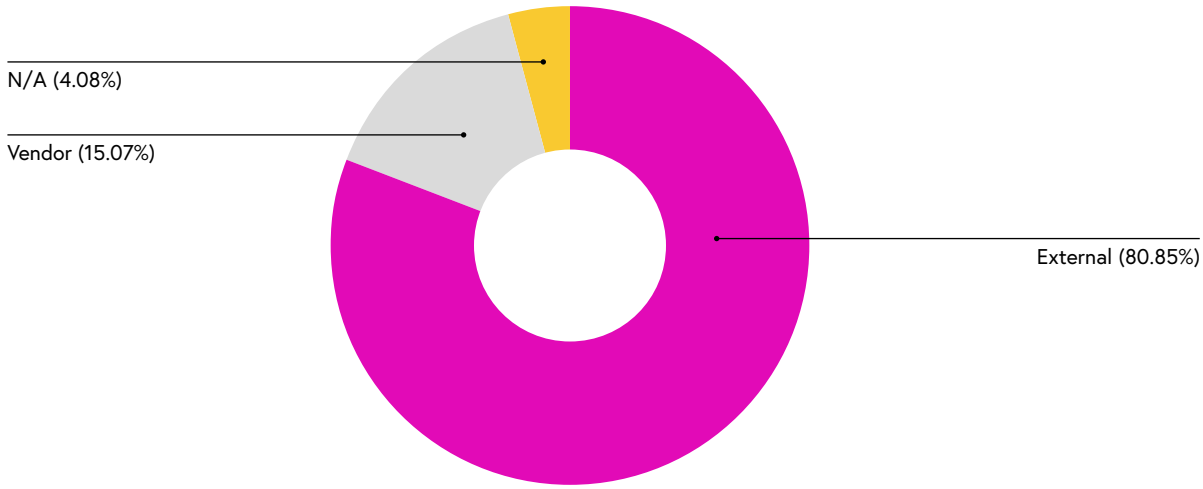



Figure 2.2a: Breakdown of vulnerabilities by origin of discovery.

The chart below breaks down the number of vulnerabilities disclosed by external sources, led by third-party companies, which found **341** vulnerabilities **(53.87%)** in 1H 2021. 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 1H 2021, this accounts for **139** vulnerabilities).

## RESEARCH GROUP

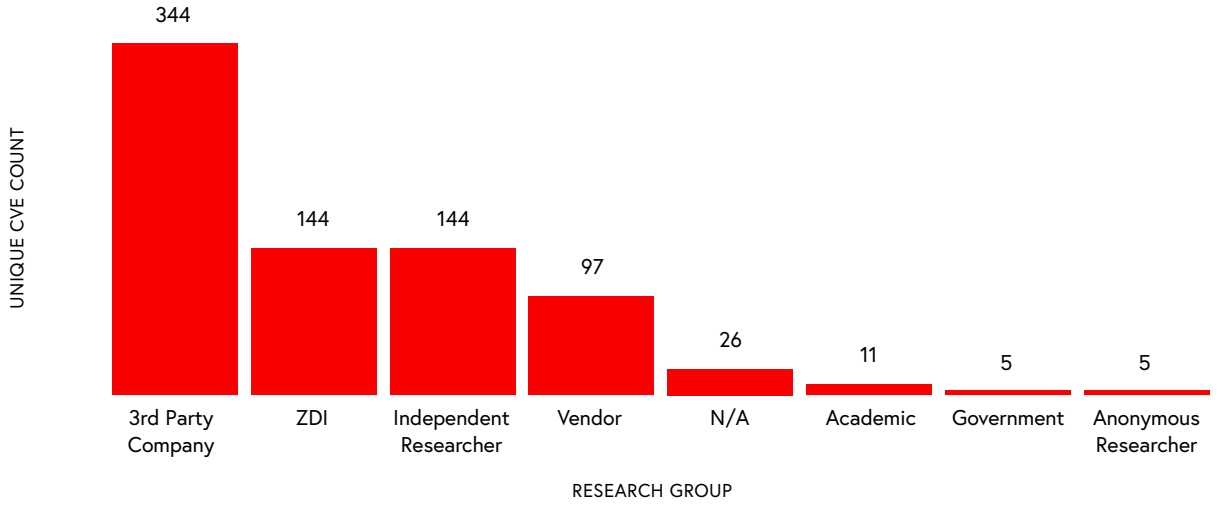



Figure 2.2b: Breakdown of vulnerability discoveries by research group.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

Note the number of disclosures coming from the Zero Day Initiative (ZDI), a third-party company that works with researchers and offers rewards for zero-day vulnerability reports. Disclosures made through ZDI in the 1H of 2021 more than doubled from all of 2020, as seen below. In 1H 2021, ZDI was involved in 22.6% of the vulnerabilities disclosed, a significant increase in comparison to previous years:

- During 1H 2021, ZDI was involved in **22.6%** of ICS vulnerabilities disclosed
- During all of 2020, ZDI was involved in **11.08%** of disclosed vulnerabilities
- During all of 2019, ZDI was involved in **12%** of disclosed vulnerabilities
- During all of 2018, ZDI was involved in **16.81%** of disclosed vulnerabilities

## Team82 also notes there were 42 new researchers reporting vulnerabilities during 1H 2021; the data in the chart below breaks down those new entrants by type.

Team82's data indicates that the new researchers focused largely on market-leading vendors, such as Rockwell Automation, Schneider Electric, Siemens, and others. **Four** of the 42 new researchers introduced four newly affected vendors in 1H 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.

**NEW RESEARCHERS ONLY**

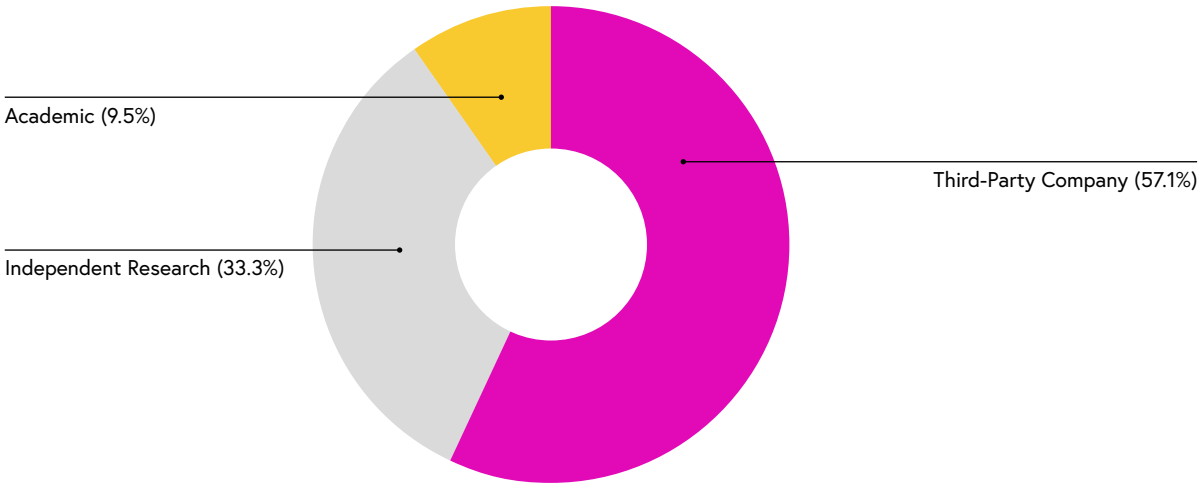



Figure 2.2c: Breakdown of new researchers reporting ICS vulnerabilities.

https://t.me/learningnets

## 2.3 AFFECTED ICS VENDORS

The **637** ICS vulnerabilities disclosed in 1H 2021 affected products from **76** vendors; the number of affected vendors is up from the 2H 2020 when there were **59** affected vendors, and **53** in the 1H 2020.

Siemens was the affected vendor with the most reported vulnerabilities at 146, many of which were disclosed as part of internal research conducted by the Siemens CERT team, followed by Schneider Electric, Rockwell Automation, WAGO, 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 a 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.

### TOP 5 AFFECTED VENDORS

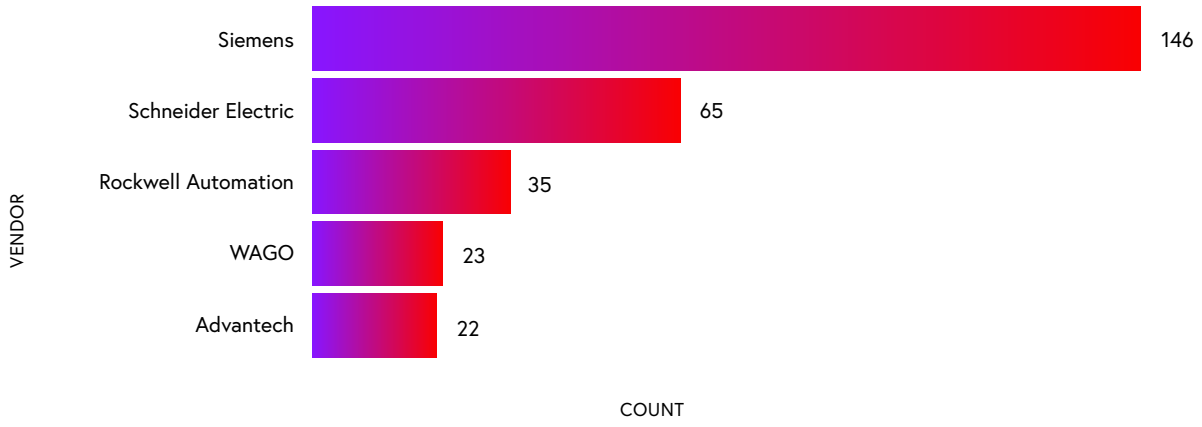



Figure 2.3a: Top five vendors affected by vulnerabilities.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## 2.4 ICS VENDORS WITH FIRST-TIME VULNERABILITY DISCLOSURES IN 1H 2021

During 1H 2021, 20 vendors whose products had not been affected by ICS vulnerabilities disclosed in 2020 were affected by at least one ICS vulnerability disclosed in 1H 2021.

- Six of these vendors specialize in medical technology, three in automation, and two in manufacturing
- Vulnerabilities affecting these newly affected vendors (16 of 20) were uncovered by researchers who had previously disclosed flaws.

| Vendors | Primary Industry |
|---|---|
| Claroty | Industrial Cybersecurity |
| ThroughTek | IoT & M2M solutions for surveillance |
| AGG Software | data acquisition, data logging, and monitoring software |
| ZOLL | Medical |
| Hillrom | Medical |
| GENIVI Alliance | Automotive |
| Mesa Labs | Medical |
| Datakit | CAD data exchange |
| Unified Automation GmbH | Industrial Automation |
| Cassia Networks | Bluetooth IoT |
| EIPStackGroup | Open Source EtherNet/IP |
| JTEKT Corporation | Automotive |
| Ovarro | Industrial Automation |
| Weintek | Industrial Automation |
| PerFact | Information Technology |
| Luxion | Lighting Technology |
| Hamilton Medical AG | Medical |
| Hilscher Gesellschaft fur Systemautomation mbH | Manufacturing |
| SOOIL Developments Co. Ltd. | Medical |
| Innokas Medical | Medical |

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## 2.5 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 include both. In 1H 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.

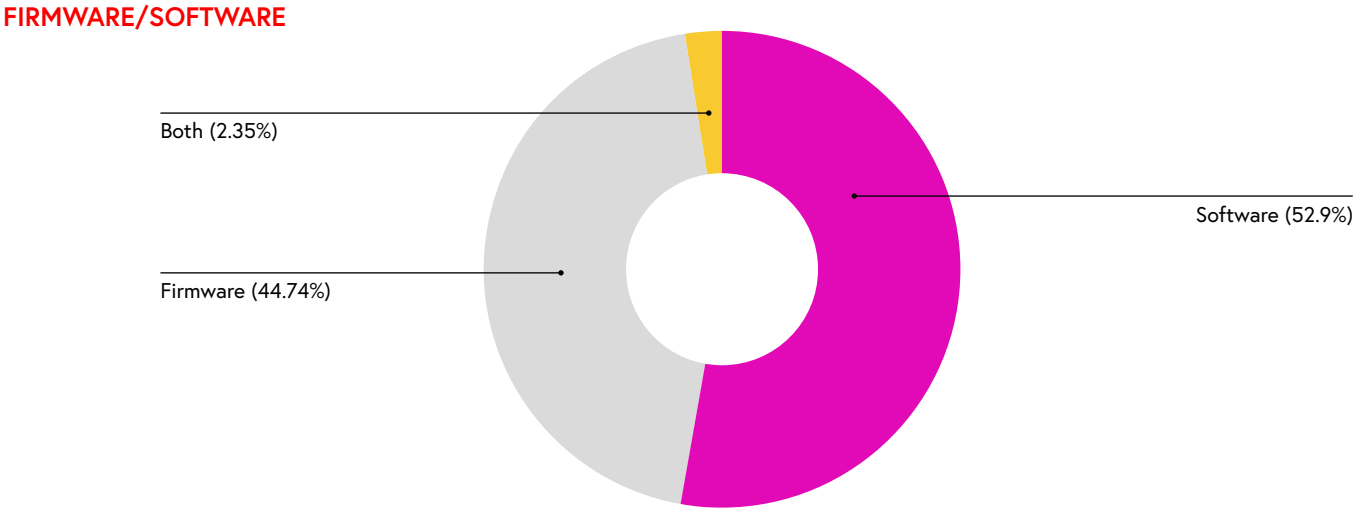



Figure 2.5a: Breakdown of vulnerabilities found in software and firmware.

## 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 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 as seen below:

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## AFFECTED PRODUCT FAMILIES

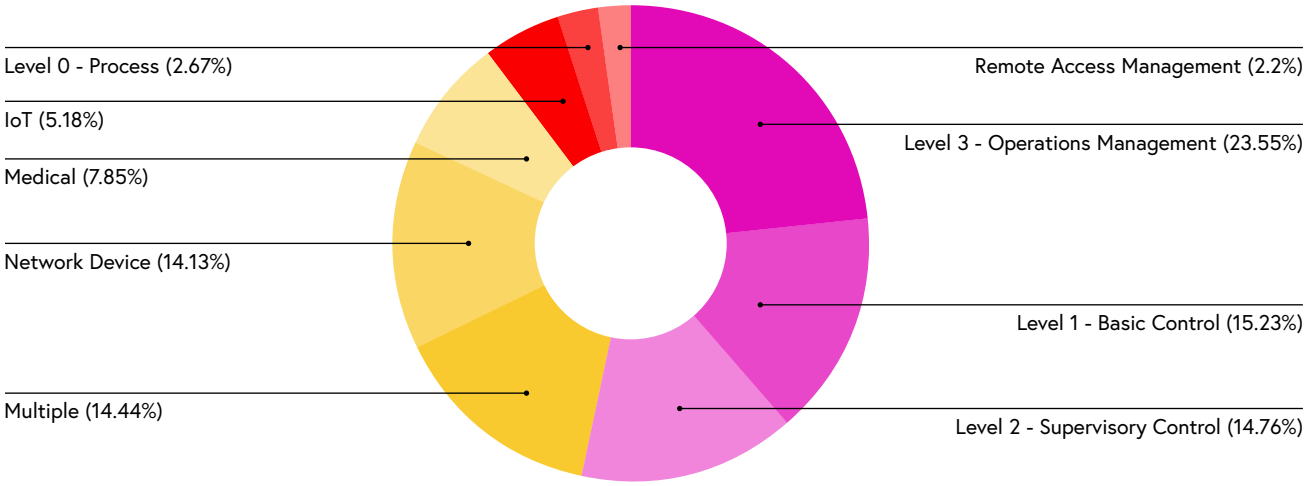



Figure 2.5b: Breakdown of affected product families.

Since **23.55%** 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 **30%** 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.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

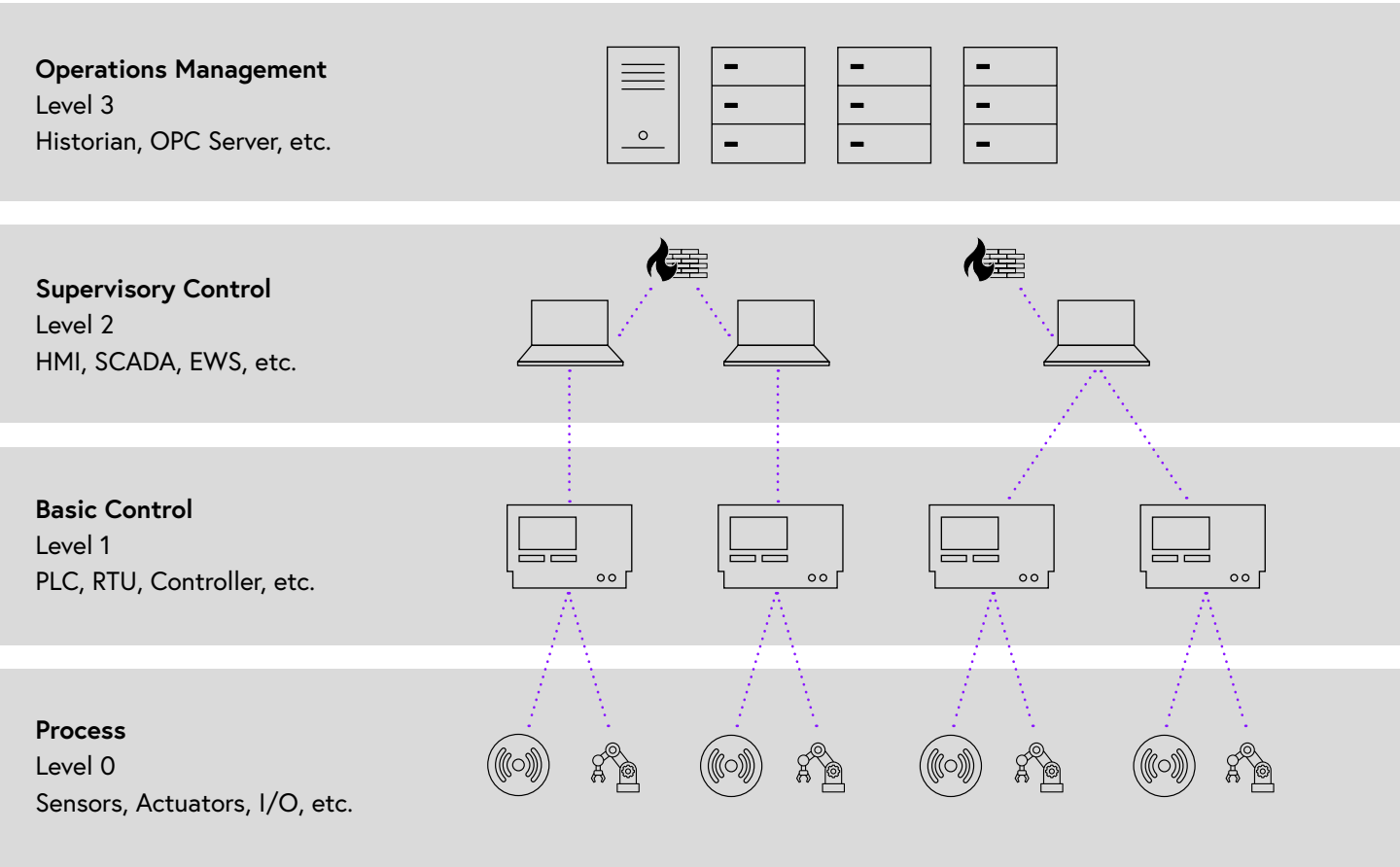



Figure 2.5c: Levels 0-3 of the Purdue Model for industrial control systems.

We want to note the Multiple category in Figure 2.5b—this category mostly contains third-party component vulnerabilities (we had many of these during the past year), which often come in bundles of multiple vulnerabilities in each disclosure. They often affect many vendors and products, and emphasize that employing protection and mitigations against third-party vulnerabilities, starting with visibility and risk assessments, 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 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 as it connects directly to the Basic Control level.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## FIRMWARE/SOFTWARE DIVISION IN PRODUCT FAMILY

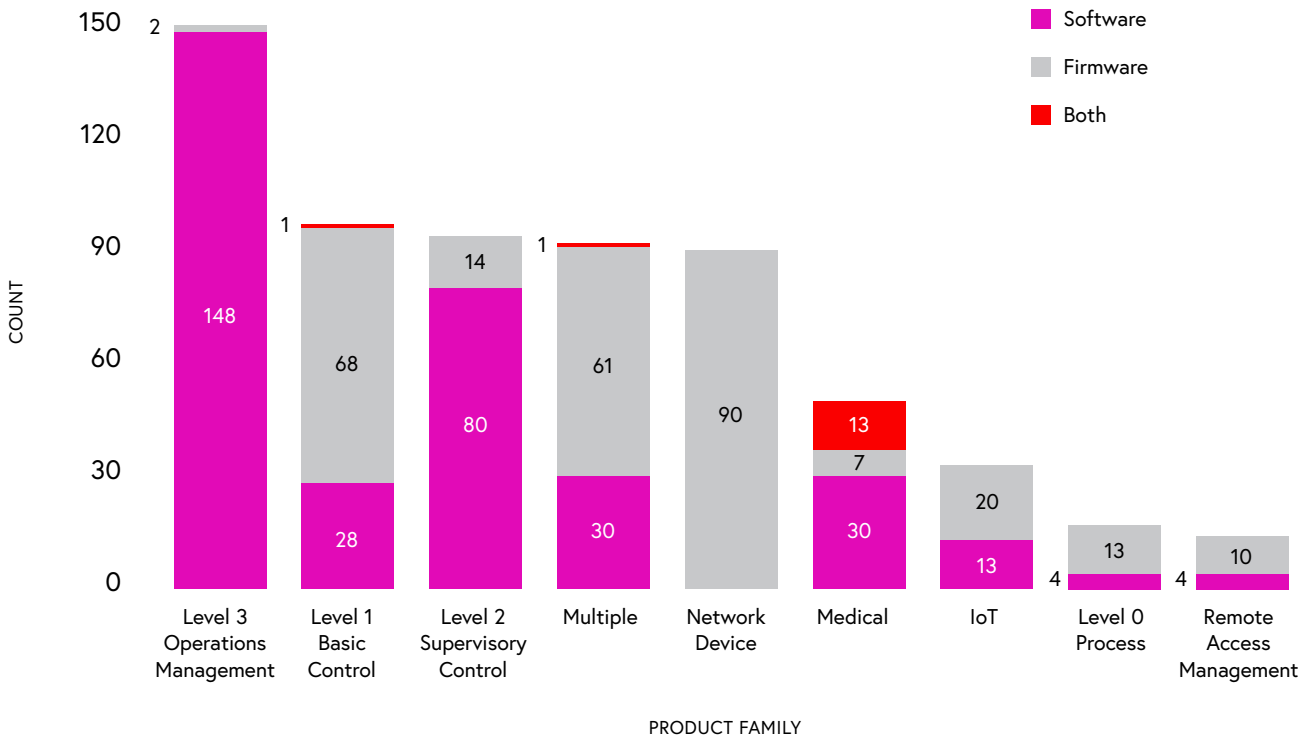



Figure 2.5d: Breakdown of firmware and software vulnerabilities by product family.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# 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 earlier. Yet despite defenders' dependence on mitigations, vendor advisories or alerts from 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, below, bears this out. For example, network segmentation and secure remote access are the top two steps, and should be top considerations for defenders ahead of other options on our list, including traffic restriction, user- and role-based policies, and the principle of least privilege.

---

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## TOP MITIGATION STEPS

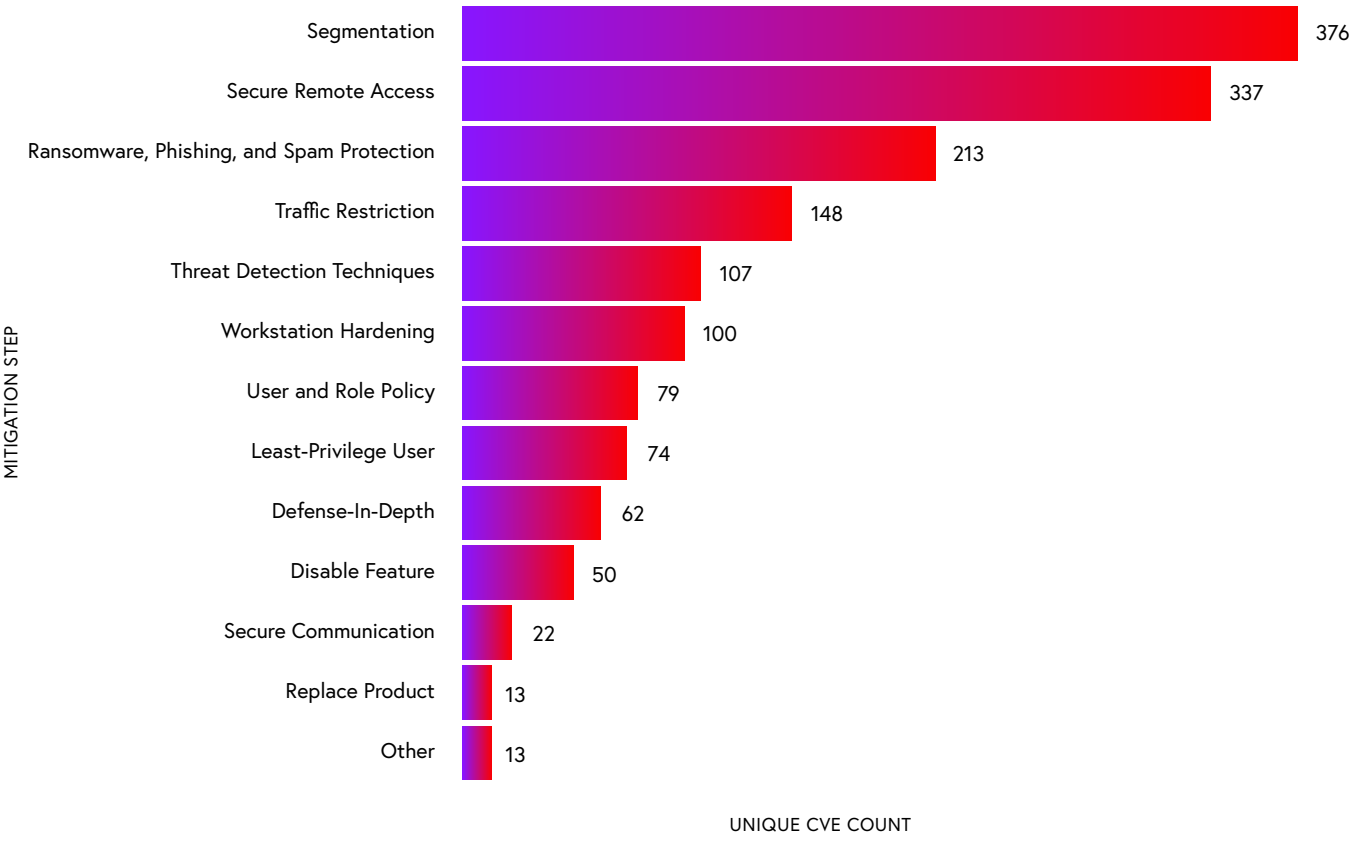



Figure 3.1a: Breakdown of top mitigation steps.

OT network segmentation is an important control as air-gaps become a relic of the past and perimeters erode with enterprises moving data, applications, infrastructure, and services to the cloud. Segmentation likely involves virtual zoning that allows for zone-specific policies that are 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.

Secure remote access was right behind segmentation as a top mitigation step. As the Oldsmar incident demonstrated, proper access controls and privilege management are crucial as companies manage a long-term trend toward remote work. Secure remote access solutions must not only alert on suspicious activities, but also provide the capability to investigate specific sessions, either live or on-demand, and allow administrators to respond by either disconnecting a session or taking another action to contain or remediate damage.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## 3.2 REMEDIATIONS

Of the 637 ICS vulnerabilities disclosed in the 1H 2021, **25.59%** have either no available fix, or a partial remediation; **13.5%** — affecting 17 vendors — have **no** remediation, and **12.1%** — affecting 12 vendors — have **partial** remediation, meaning not all affected products have a fix available.

- Of the vulnerabilities with no, or partial, remediation, **61.96%** were found in firmware (another 4.29% were found in both software or firmware); the products are mostly deployed across network devices (37.62%) and Level 1 Basic Control (19.8%) of the Purdue Model.
- Of the vulnerabilities with no, or partial, remediation, **55.21%** when exploited, could result in remote code execution
- Of the vulnerabilities with no, or partial, remediation, **47.85%** when exploited, could result in denial-of-service attacks; some vulnerabilities here and above could have multiple impacts, leading to either remote code execution and denial of service, for example.

For **74.4%** of the 637 vulnerabilities affecting 70 vendors, there is remediation. The majority (59.5%) of the updates are software fixes (there's another 1.69% that were found in both software and firmware) emphasizing again that given the comparative ease in patching software over firmware, defenders have the ability to prioritize patching within their environments.

When looking into the products for which there is a software fix, the majority **(51.42%)** are in Level 3: Operations Management, followed by Level 2: Supervisory Control **(19.86%)**.

### AFFECTED PRODUCTS FAMILIES

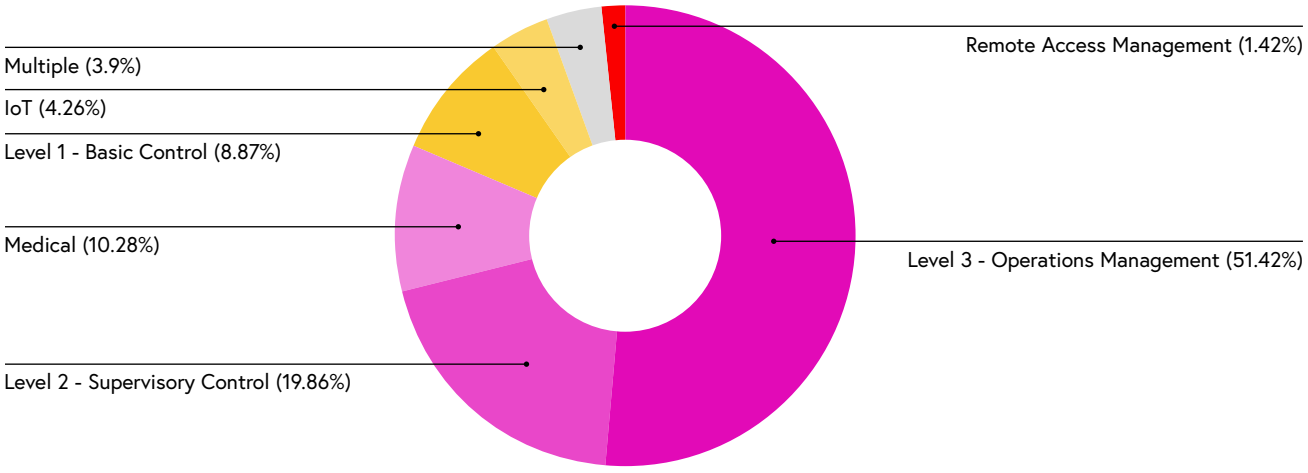



Figure 3.2a: Breakdown of software remediation availability by product family.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

As for firmware, it seems that in addition to the inability to patch over time, there is also the issue of having fewer remediation solutions available. When firmware remediations do exist, Team82's data shows that it is for a majority of network devices (**28.26%**), below, followed by Level 1: Basic Control (**26.09%**). This demonstrates that even in firmware, some prioritization of updates could happen because updating a network device, for example a switch, is easier and likelier than upgrading a PLC or an RTU.

## AFFECTED PRODUCTS FAMILIES

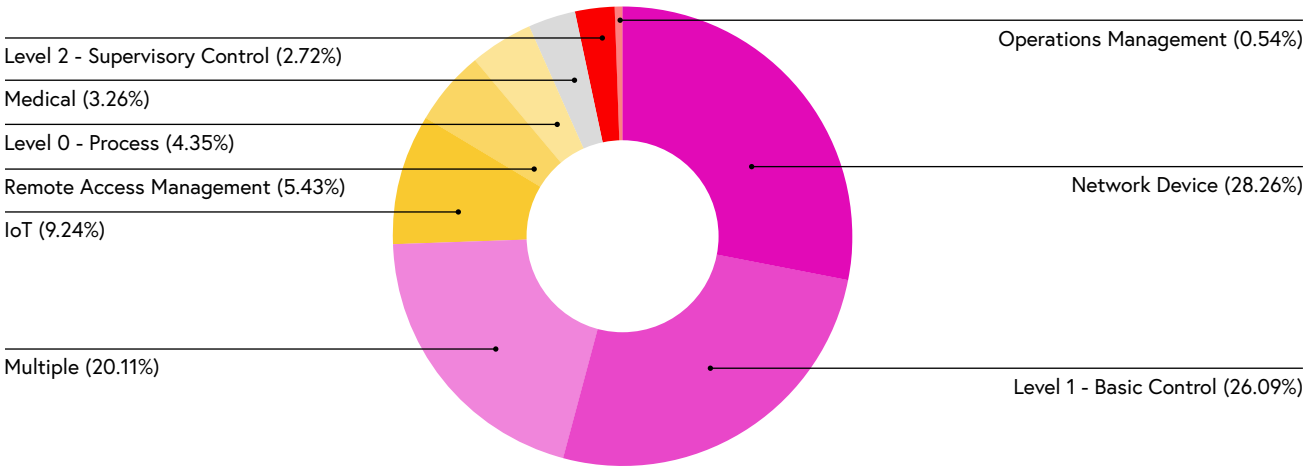



Figure 3.2b: Breakdown of firmware remediation availability by product family.

## 3.3 END-OF-LIFE PRODUCTS

Of the 637 vulnerabilities, 6.43% affect end-of-life products for which there is no remediation planned because the vendor no longer supports them.

- 51.22% of those vulnerabilities were found in firmware (another 14.63% that were found in both software or firmware).
- As seen below, these end-of-life products are deployed across various levels of the network:

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## AFFECTED PRODUCTS FAMILIES

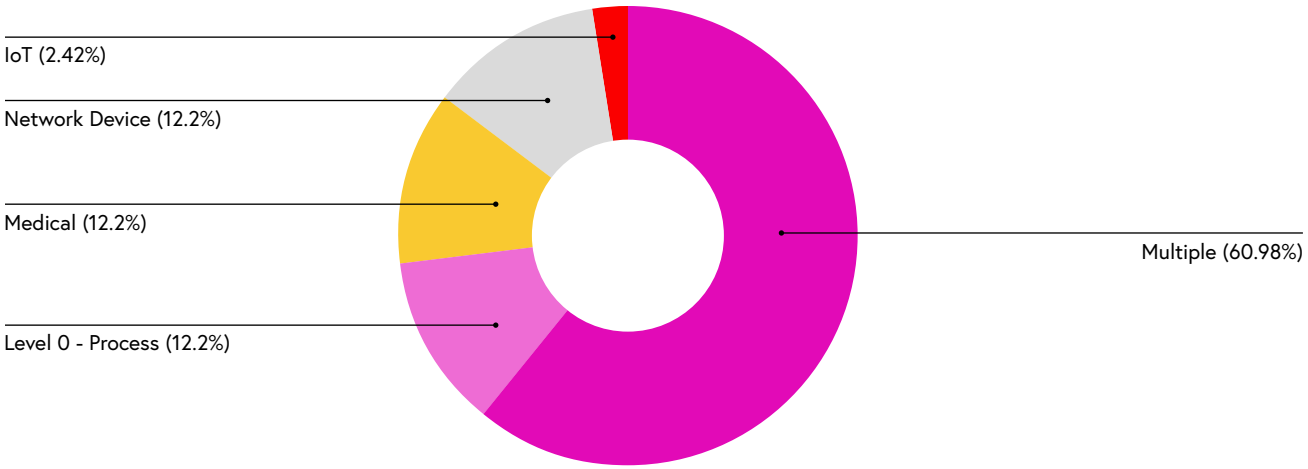



Figure 3.3a: Breakdown of affected end-of-life products.

- **97.56%** of the vulnerabilities affecting end-of-life products are exploitable remotely via a network attack vector.
- **63.41%** of the vulnerabilities, when exploited, could lead to remote code execution.
- **24.39%** of the vulnerabilities, when exploited, could lead to denial of service.

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; firmware updates could take months and sometimes years to be developed and distributed. That along with having fewer remediation solutions lead to the understanding that defenders mostly depend on mitigations.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# PART 4: CVSS INFORMATION

The Common Vulnerability Scoring System (CVSS) comprises 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.

## 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, **61.38%** of the vulnerabilities are remotely exploitable through a network attack vector. This emphasizes the importance of protecting remote access connections and internet-facing ICS devices. Despite still being the major attack vector, this number is a decrease from 2H 2020 (down from 71.49%) because we saw a rise in local attack vectors.

As for vulnerabilities with a local attack vector, in **72.14%** 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; attacks exploiting such techniques are on a rise and users should adhere to security measures explained in the Recommendations section of this report.

### ATTACK VECTOR DISTRIBUTION

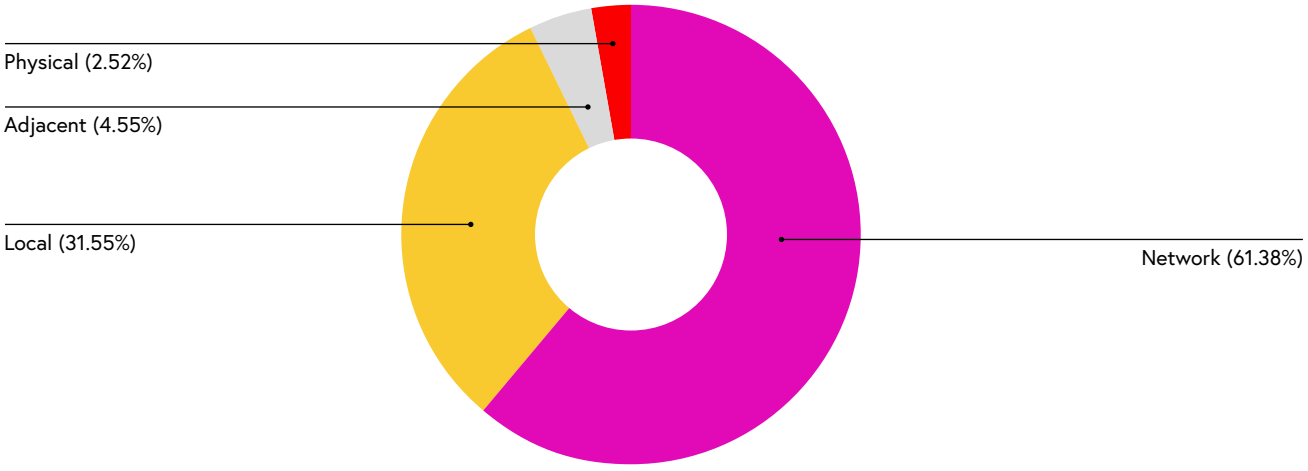



Figure 4.1a: Attack vectors associated with ICS vulnerabilities

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

The local attack vector is mostly dominant in the Operations Management and Supervisory Control levels. Moreover, in **94.38%** of the Operations Management vulnerabilities via a local attack vector, user interaction is required for exploitation.

An attacker's dependence on user interaction shows the importance of awareness and protection against social engineering tactics among workers with access to critical assets.

## ATTACK VECTOR PER PRODUCT FAMILY

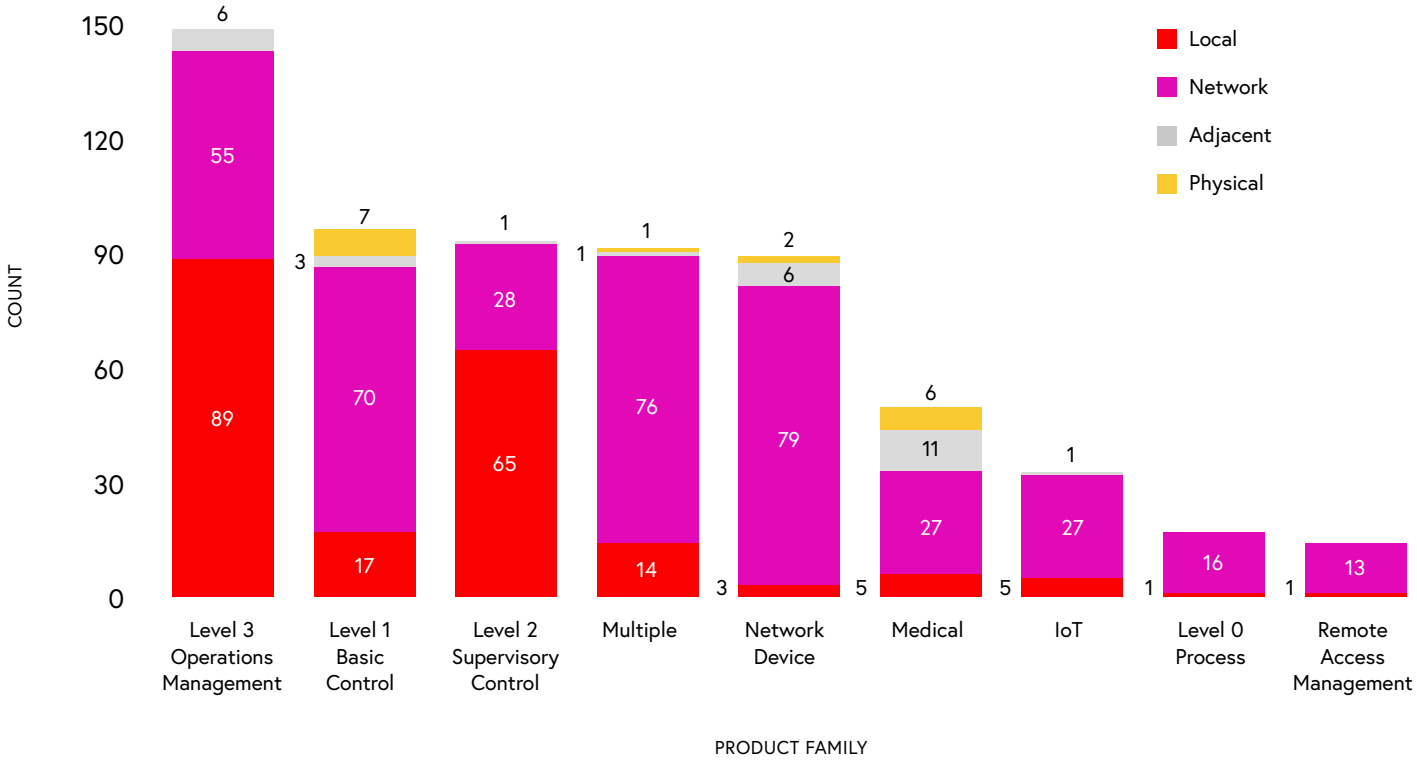



Figure 4.1b: Attack vectors by product family.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

### 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 **89.64%** of the vulnerabilities, the complexity of exploitation is considered low, meaning these vulnerabilities don't require special conditions and an attacker can expect repeatable success every time.

## CVSS ATTACK COMPLEXITY

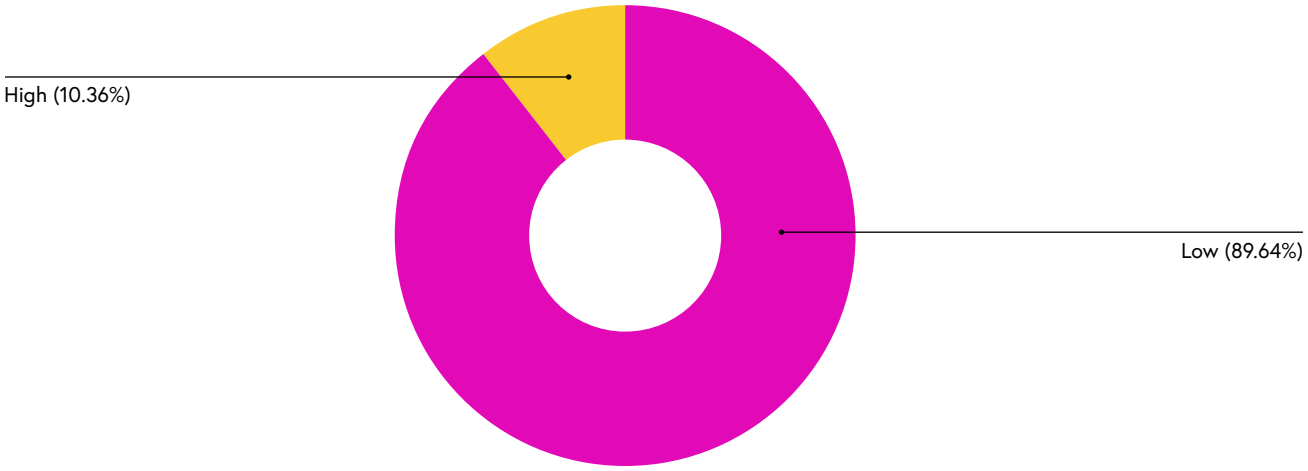



Figure 4.1c: Attack complexity according to CVSS scoring.

## 4.2 PRIVILEGES REQUIRED

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

As you can see in the following graph, for **73.78%** of the vulnerabilities, the attacker is unauthorized prior to attack and doesn't require any access to settings or files of the target.

https://t.me/learningnets

## CVSS PRIVILEGES REQUIRED

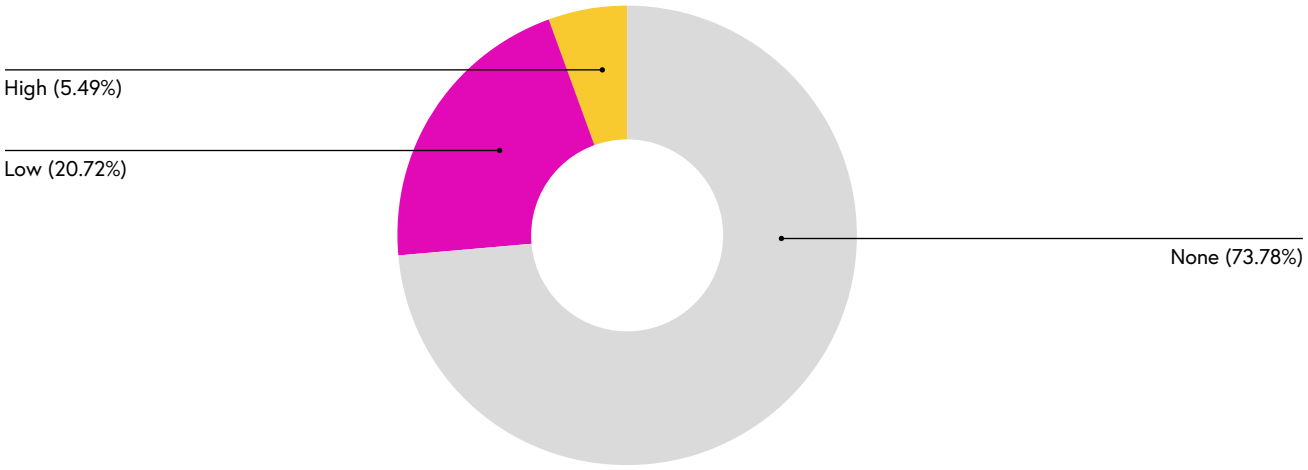



Figure 4.2a: Privileges required to exploit vulnerabilities.

### USER INTERACTION

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

As you can see in the following graph, for **66.25%** of the vulnerabilities, there is no requirement for user interaction.

## CVSS USER INTERACTION

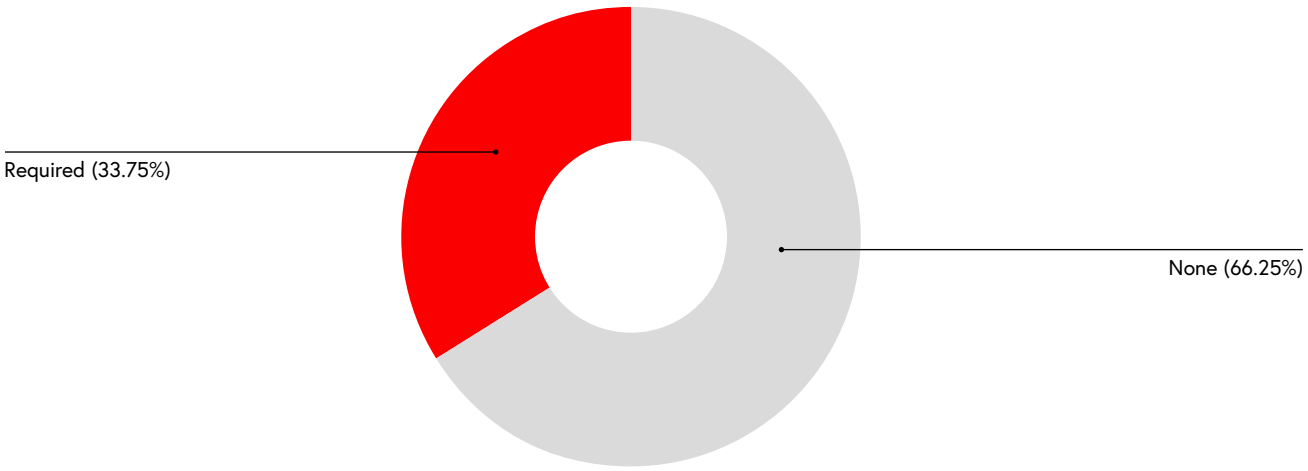



Figure 4.2b: User interaction required by exploit vulnerabilities.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## 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.

### 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 94.5% of the vulnerabilities. A reminder, as mentioned above, that while confidentiality is important in IT security, it acts as a far less significant risk variable in OT networks.

### CVSS CONFIDENTIALITY

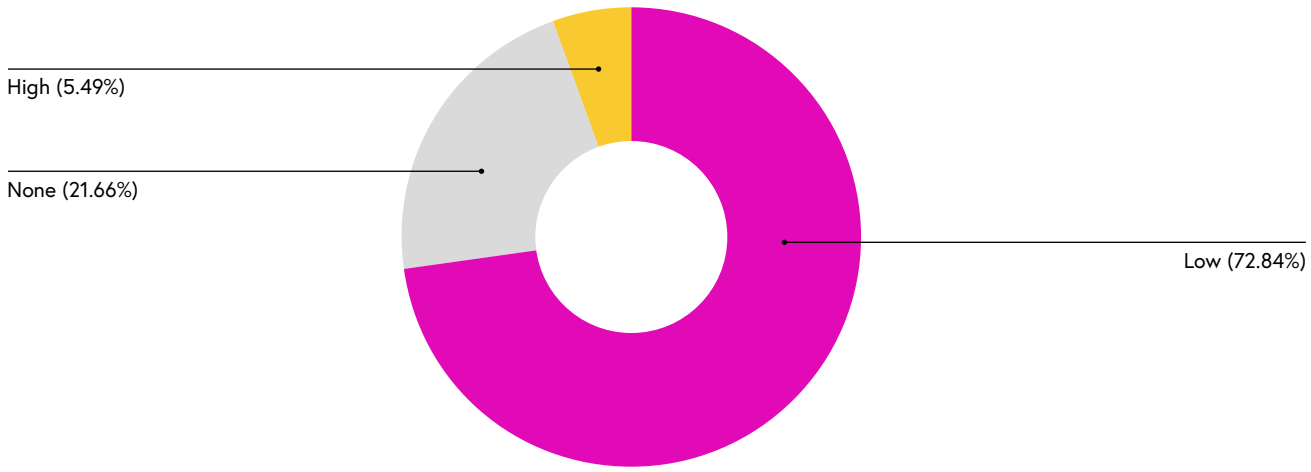



Figure 4.3a: Impact to confidentiality.

https://t.me/learningnets

### 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 **69.7%** of the vulnerabilities, the impact to integrity is none whatsoever. Again, as mentioned above, it shows that while integrity of information is important in IT security, it is a lesser risk variable in OT networks.

## CVSS INTEGRITY

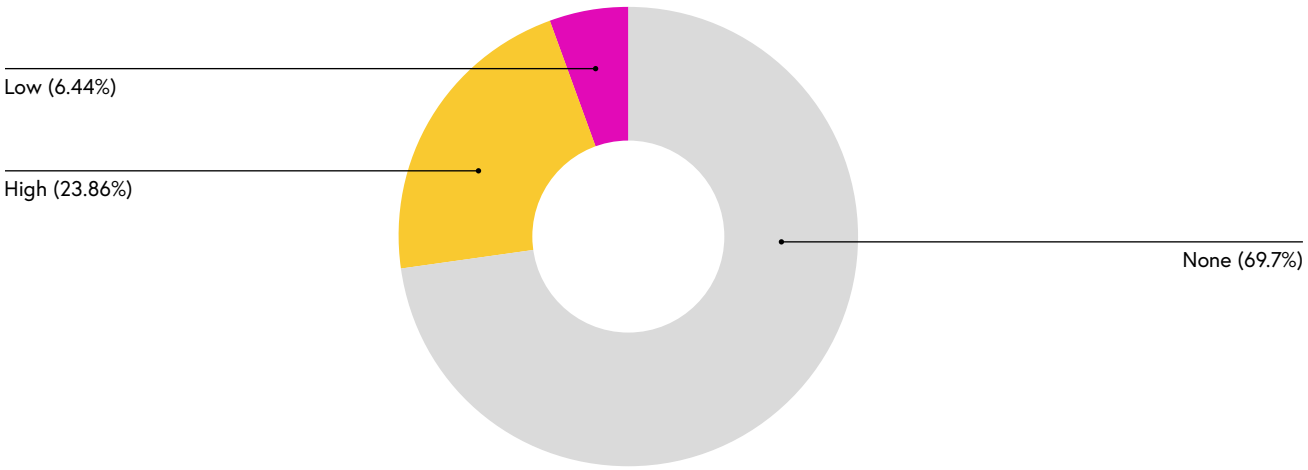



Figure 4.3a: Impact to confidentiality.

### 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% 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.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## CVSS AVAILABILITY

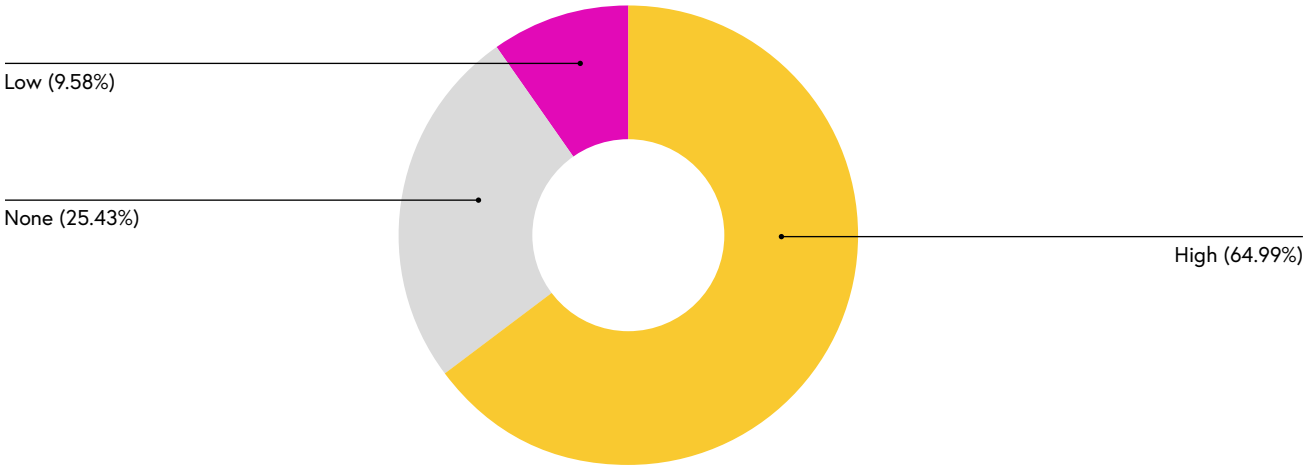



Figure 4.3c: Impact to availability.

## 4.4 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 87.28% 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

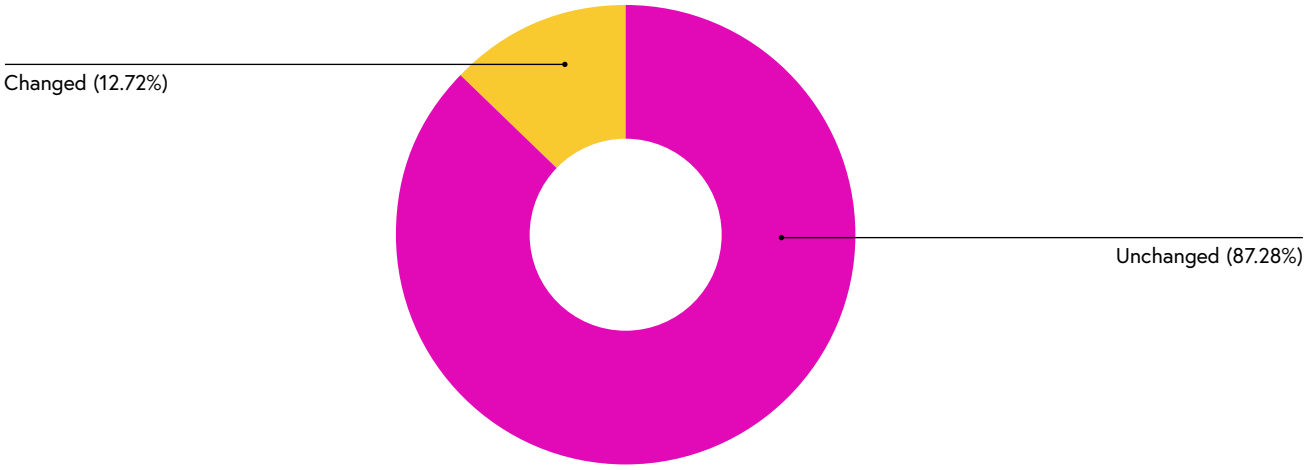



Figure 4.4a: CVSS scope

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## 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.

**70.64%** of ICS vulnerabilities were 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

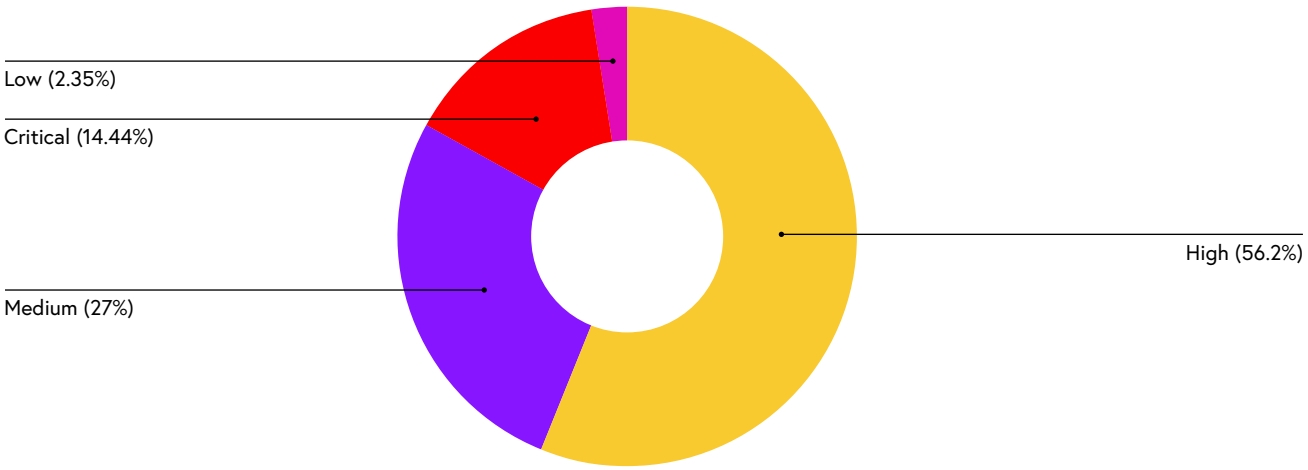



Figure 4.5a: Breakdown of CVSS scores by criticality.

https://t.me/learningnets

# PART 5: EXPLOITED CWEs

Security weaknesses—or Common Weakness Enumerations (CWEs)—manifested in the ICS vulnerabilities disclosed during 1H 2021 help explain why most of these vulnerabilities have CVSS scores categorized as either high or critical.

**The top five most prevalent CWEs** from Team82's data are prominent on The MITRE Corporation'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.

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 buffer's bounds or when pointer arithmetic results in a position outside of a valid memory location. Successful exploitation can result in data corruption, denial-of-service, or code execution.

- This CWE manifests in **11.5%** of vulnerabilities, up from **6.74%** in 2H 2020.
- This CWE is No. 1 on MITRE's 2021 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 **5.68%** of the vulnerabilities, up from **5.65%** in 2H 2020.
- This CWE is No. 3 on MITRE's 2021 Top 25 most dangerous software weaknesses.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

### CWE-20 IMPROPER INPUT VALIDATION

The product incorrectly validates or does not validate input that may affect the control flow or data flow of the program. Software that validates input improperly allows an attacker to craft input in a way that is unexpected to the rest of the software. Successful exploitation can result in control flow alterations, memory modification, DoS, or code execution.

- This CWE manifests in **3.93%** of the vulnerabilities, up from **3.85%** in 2H 2020.
- This CWE is No. 4 on MITRE's 2021 Top 25 most dangerous software errors.

### CWE-119 IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER

The software performs operations on a memory buffer, but it can read from, or write to, a memory location that is outside of the intended boundary of the buffer. Successful exploitation can result in arbitrary code execution, system crash, alteration of the intended control flow, or ability to read sensitive information.

- This CWE manifests in **3.93%** of the vulnerabilities, up from **1.93%** in 2H 2020.
- This CWE is No. 17 on MITRE's 2021 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 1H 2021 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: causing denial of service, bypassing protection mechanisms, and allowing an adversary to modify memory, or read application data.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## VULNERABILITY COUNT BY IMPACT

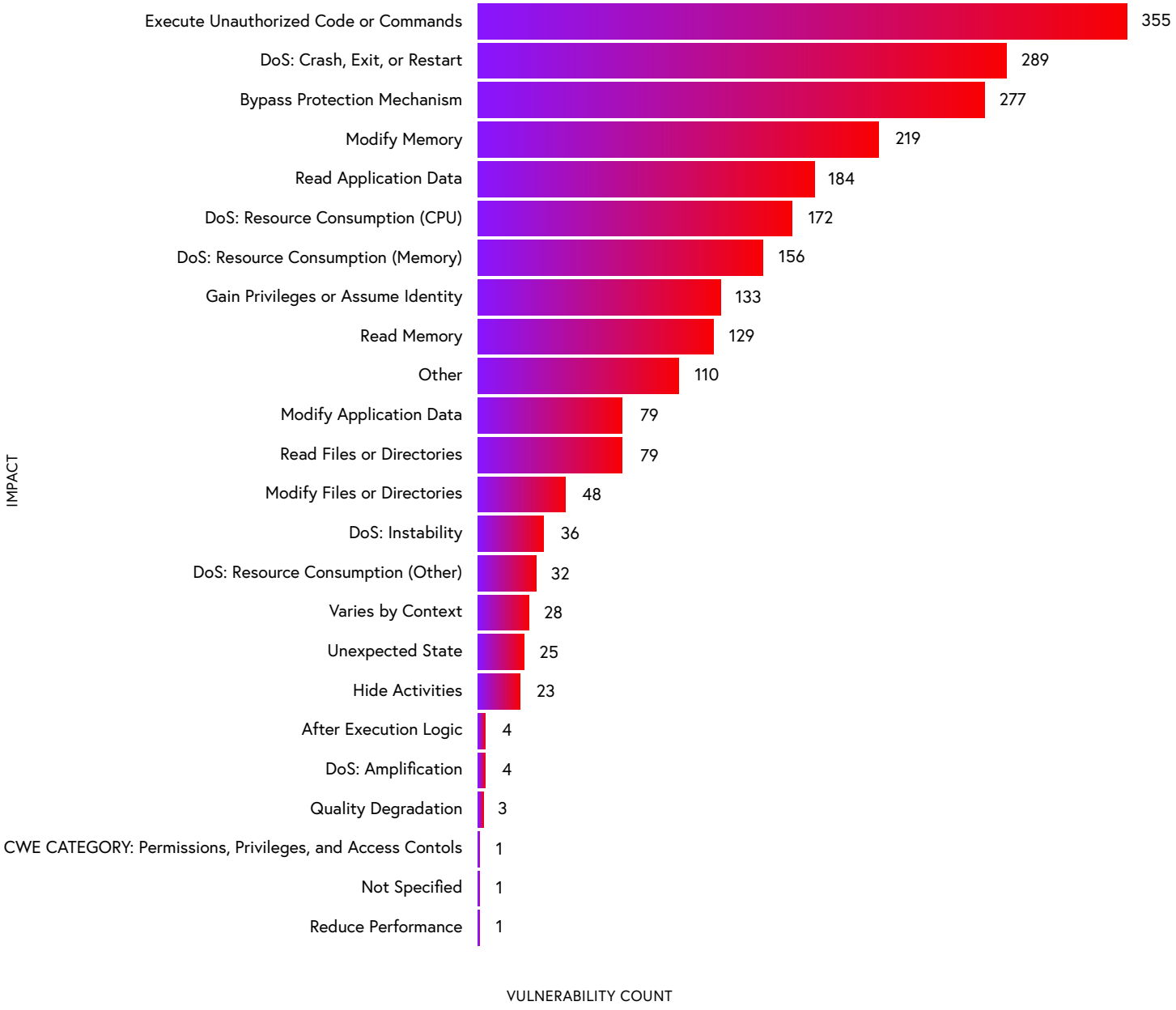



Figure 5a: Breakdown of the number of vulnerabilities by CWE impact.

A comparison of ICS vulnerability data from the 1H of 2019, 2020, and 2021 shows the longevity of remote code execution, and DoS as the top two most prevalent impacts.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

The number of vulnerabilities that could result in remote code execution saw a notable increase of **64.35%** from last year, and 74% from 1H 2019, while DoS (**+68%, +102.1%**) and bypass protection mechanisms (**+87.16%, +102.2%**), also saw significant increases from 1H 2019.

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

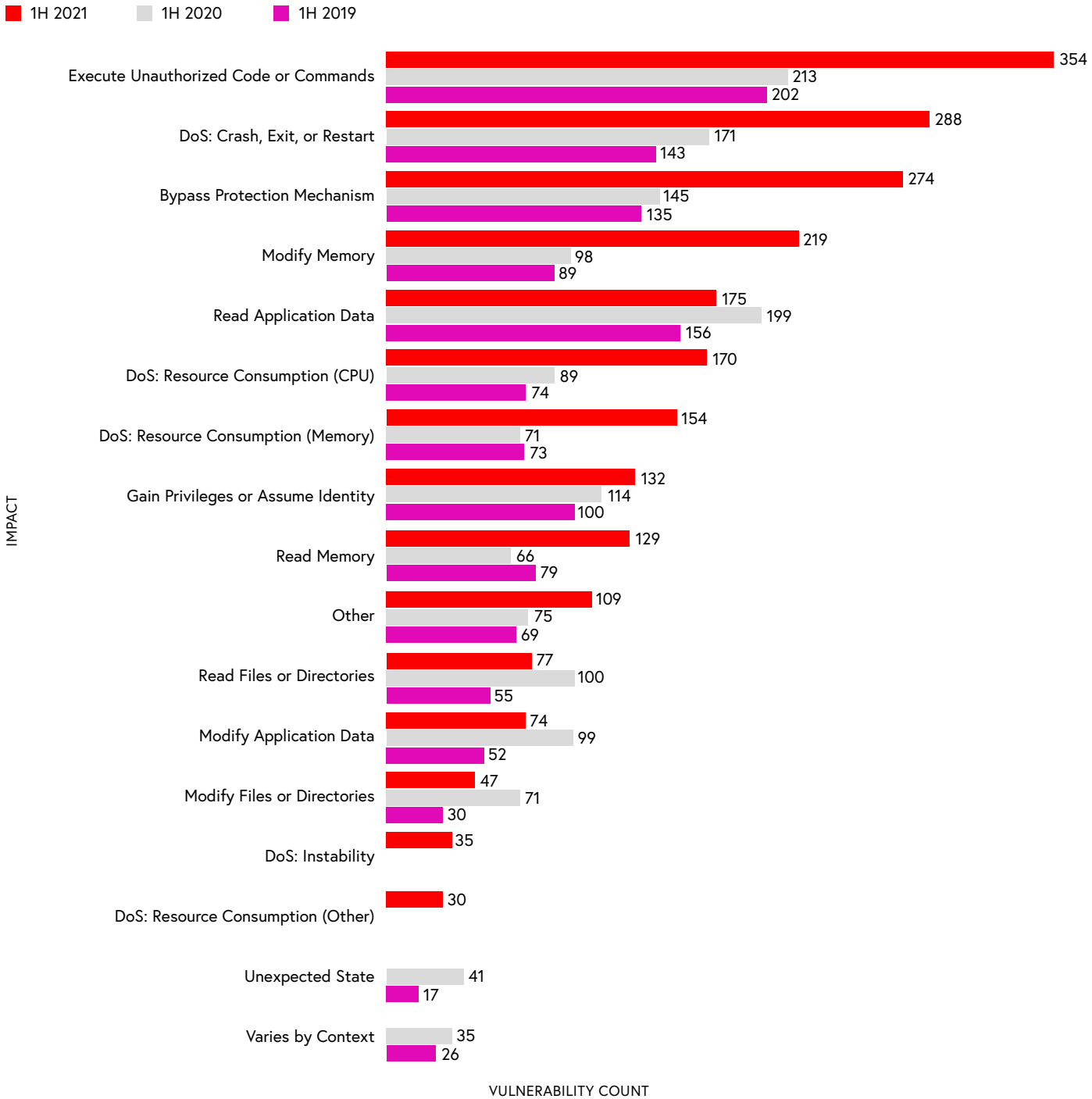



Figure 5b: Year-over-year comparison of vulnerability counts by impact.

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# PART 6: KEY EVENTS RELEVANT TO THE 1H 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 1H 2021.

## COLONIAL PIPELINE ATTACK

Colonial Pipeline, the East Coast of the United States' largest gasoline, diesel, and natural gas distributor, was attacked by ransomware, and the attack impacted oil and gas delivery. Shutting down on May 7—the first shutdown in Colonial's 57-year history—caused an immediate impact on the sector because Colonial supplies approximately 45% of the East Coast's fuel. The outage led to a rise in gasoline and home heating oil prices, and many gas stations ran out of fuel. Colonial resumed its operations on May 13.

DarkSide, a Russian cybercrime group that sells ransomware as a service (RaaS), was alleged to be responsible for the attack. DarkSide steals sensitive data and extorts victims with threats of publishing it if a ransom demand is not met. Based on previous reports, DarkSide seemed to seek out only victims capable of paying exorbitant ransom demands and they claimed to not target healthcare organizations, education, or government agencies. Colonial paid a $4.4M ransom in Bitcoin ($2.3M of it was recovered by the U.S.), however, shortly after the attack, DarkSide reportedly abandoned its operation.

For further information regarding the Colonial Pipelines attack, refer to:
https://claroty.com/2021/05/10/blog-research-colonial-pipeline/

## OLDSMAR WATER HACK

On Feb. 5, a water treatment facility in Oldsmar, Fla., was attacked. Operators inside the Oldsmar facility detected two intrusions from outside the plant, the second of which involved a remote attacker, who connected via TeamViewer desktop-sharing software, a legitimate remote access solution used for technical support.

The remote attacker changed levels of sodium hydroxide in residential and commercial drinking water from 100 parts-per-million to 11,100 parts-per-million. Sodium hydroxide, or lye, is added to water to control acidity and remove certain metals. Lye is also the primary agent in drain cleaners and is a caustic substance that is dangerous if consumed.

The operators cut off the attacker's access, and supported by safeguards innate to water-treatment systems, kept the contaminated water from ever reaching the public.

For further information regarding the Oldsmar attack, refer to:
https://www.claroty.com/2021/02/16/blog-research-oldsmar-water-hack-highlights-systemic-problems-undermining-critical-infrastructure/

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## JBS FOODS ATTACK

JBS, the world's largest meat supplier, was attacked by ransomware on May 30, leading to a shutdown of plants in Australia, Canada and the U.S. The shutdown in the United States wiped out nearly one-fifth of the U.S. plants' meat-processing capacity. The FBI attributed the attack to REvil, also known as Sodinokibi.

REvil is a hacker group providing RaaS. They are known for extorting large ransoms, targeting big corporations, and stealing data before encryption for double extortion, which they post on a site on the dark web called "Happy Blog."

JBS maintains a backup system and was able to resume operations using it to restore the data. Regardless, the company reportedly paid the attackers an $11 million ransom in order to recover.

For further information regarding the JBS attack, refer to:
https://claroty.com/2021/06/02/blog-jbs-attack-puts-food-and-beverage-cybersecurity-to-the-test/

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# 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 configure in such a way that 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

## REMOTE ACCESS CONNECTIONS PROTECTION

Remote workforces are the new normal, even as the world begins to emerge from the restrictions imposed during the COVID-19 pandemic. As organizations adjust to 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
- Enforce multi-factor authentication

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

## 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. Users should adhere to the following recommendations:

- 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

## PROTECTING OPERATIONS MANAGEMENT AND BASIC & SUPERVISORY CONTROL

The majority of ICS and SCADA vulnerabilities disclosed during 1H 2021 affected Level 3: Operations Management (Historian, OPC Server, etc.) followed by the Level 1: Basic Control (controllers, PLCs, RTUs) and 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

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved

# ACKNOWLEDGEMENTS

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

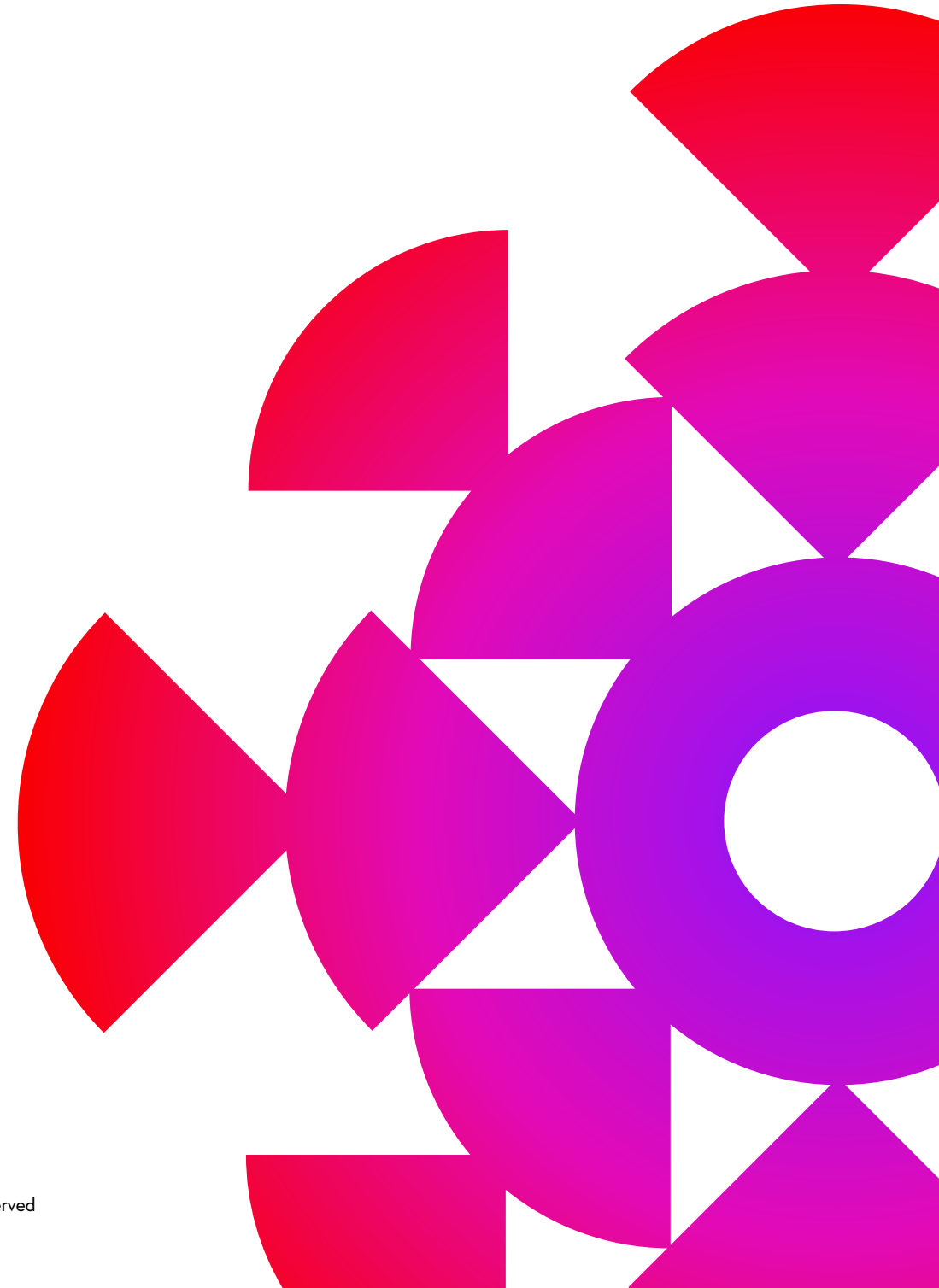
Contributors include: Rotem Mesika, security research team lead at Claroty, Nadav Erez, director of innovation, Sharon Brizinov, vulnerability research team leader, and Amir Preminger, vice president of research at Claroty. Special thanks to the entire Claroty Research Team for providing exceptional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

https://t.me/learningnets
Copyright © 2021 Claroty Ltd. All rights reserved



CLAROTY

Copyright © 2021 Claroty Ltd. All rights reserved

https://t.me/learningnets