T82
THE CLAROTY RESEARCH TEAM

CLAROTY

STATE OF XIOT SECURITY

Team82's analysis of vulnerabilities impacting cyber-physical systems across the Extended Internet of Things—1H 2022

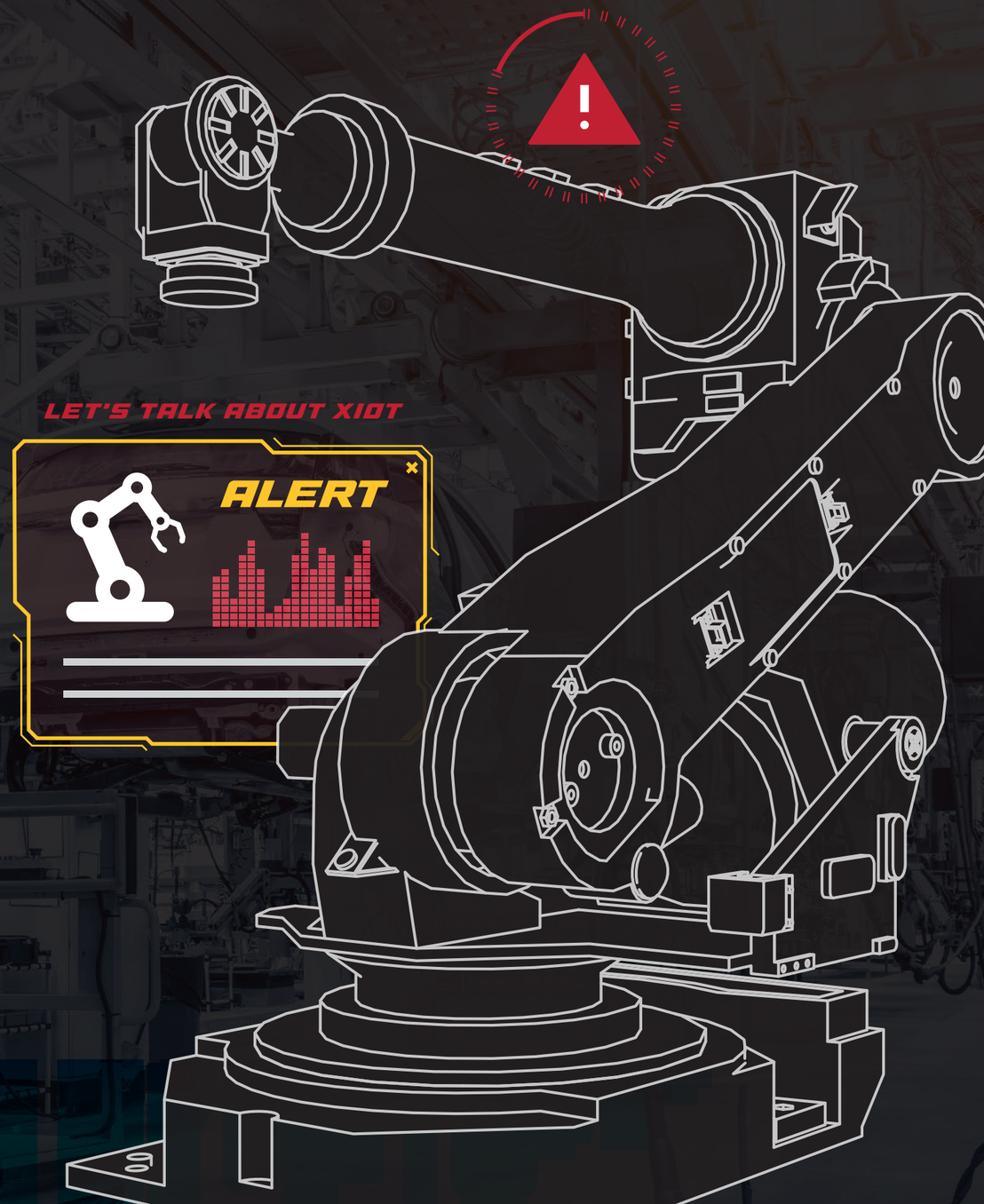
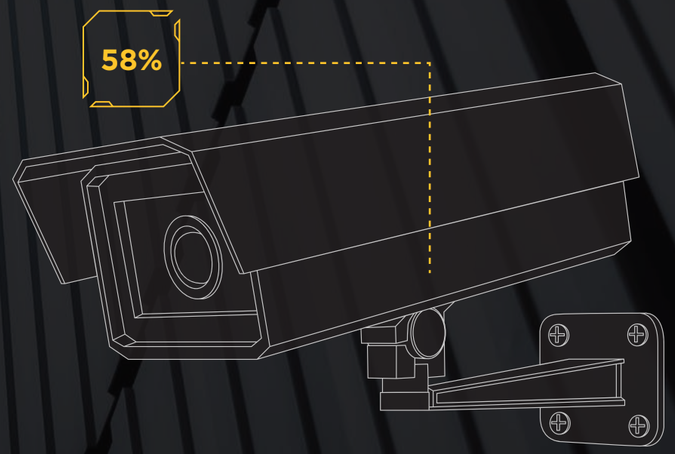
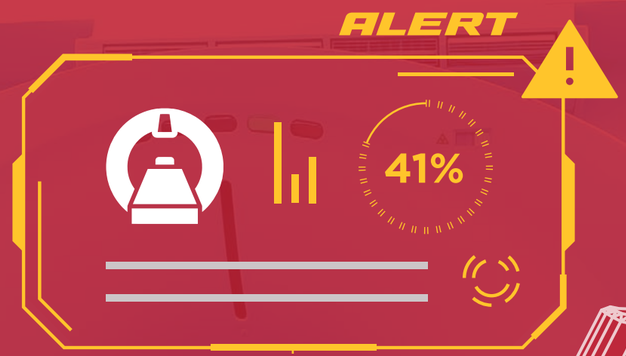


TABLE OF CONTENTS





EXECUTIVE SUMMARY

IoT Vulnerabilities Upward Bound

How Many Vulns, and How Critical?

Let's Talk About Firmware

Eyes on Vendor Self-Disclosure

EXECUTIVE SUMMARY

After more than 20 years of connecting things to the internet, we've reached a critical mass where the food we eat, water we drink, elevators we ride, and the oil and gas that warms our homes rely on computer code. Today's cyber-physical systems are directly linked to outcomes in the physical world, and despite the advances in technology that allow us to bring new efficiencies to these services, cybersecurity continues to lag.

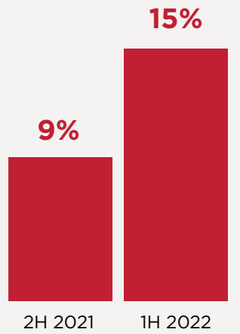
That's why we've revamped our biannual report to embrace an understanding of the vulnerabilities being disclosed and fixed within the Extended Internet of Things (XIoT), the umbrella term for connected cyber-physical devices within industrial (industrial control systems and operational technology), healthcare (connected medical devices), and commercial environments (building management systems and enterprise IoT).

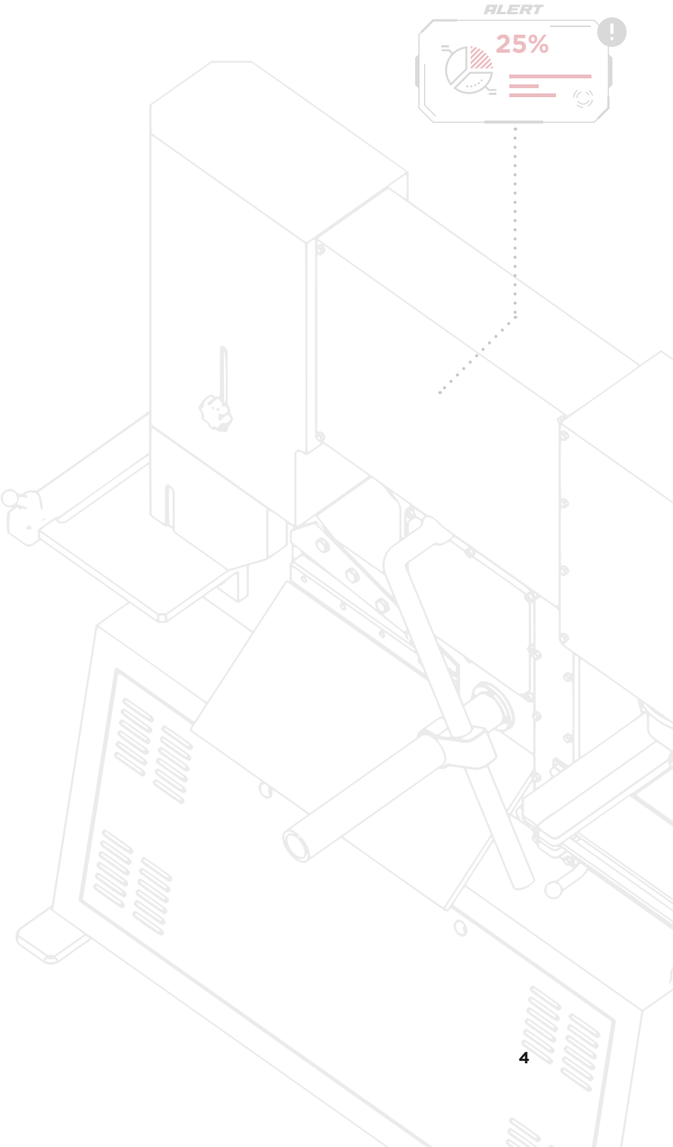
In order to properly assess risk within these critical sectors, decision makers must have a complete snapshot of the vulnerability landscape and thus prioritize and mitigate (or remediate) mission-critical systems before they impact public safety, patient health, smart grids and utilities, and more.

The State of XIoT Security report is Claroty's contextual analysis of cyber-physical security. The data presented in this edition of the report covers the first six months of 2022, and sheds light on the key trends and recommended actions you can apply within your enterprise.

Security managers, asset owners and operators, and IT analysts newly tasked with securing operational technology, IoT, connected medical devices, and building automation for example, are urged to share and use this report as a resource. The State of XIoT Security report presents not only vulnerability data, but also the necessary context around these critical issues in order to assess risk and prioritize remediation. Let's highlight some of those trends that dominated 1H 2022:

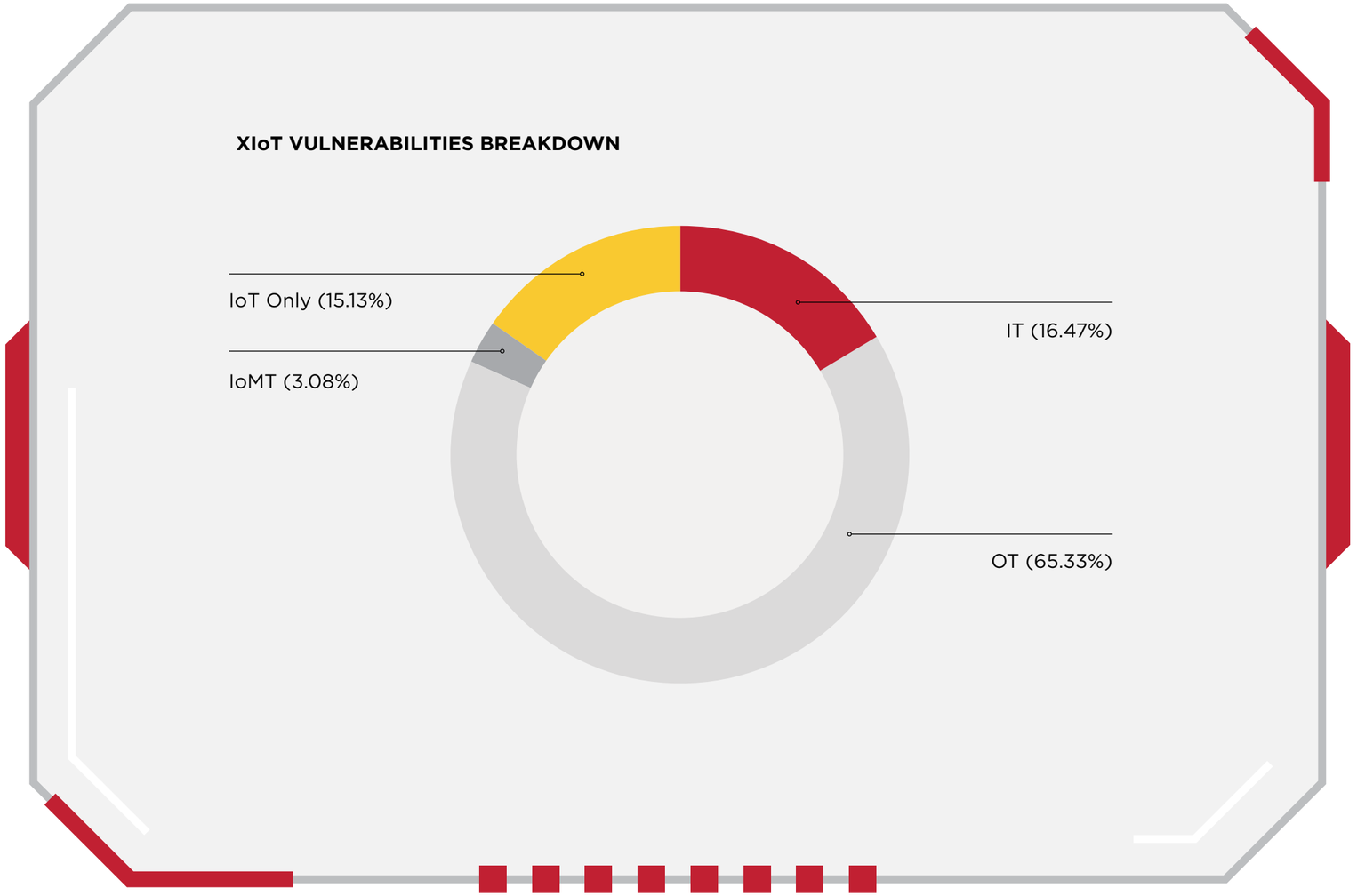
IoT VULNERABILITIES UPWARD BOUND





The numbers in the graphic, right, are quite telling. First, we see the percentage of vulnerabilities disclosed in connected, embedded internet of things (IoT) devices is 15%; that's a significant increase from Team82's last report which covered the 2H of 2021 when IoT was at 9% of all vulnerabilities.

Security researchers, whether independent or vendor-based such as Team82, and vendors themselves are deeply examining the security of connected devices. IoT devices—including surveillance cameras, routers, smart-home equipment—generally cannot support strong security technology such as encryption, or still contain factory-default credentials that can be abused to draft these devices into botnets or gain deeper network access. These numbers are significant, and indicate that companies are leaning toward patching these vulnerabilities and an interest in staying ahead of publicly available exploits.



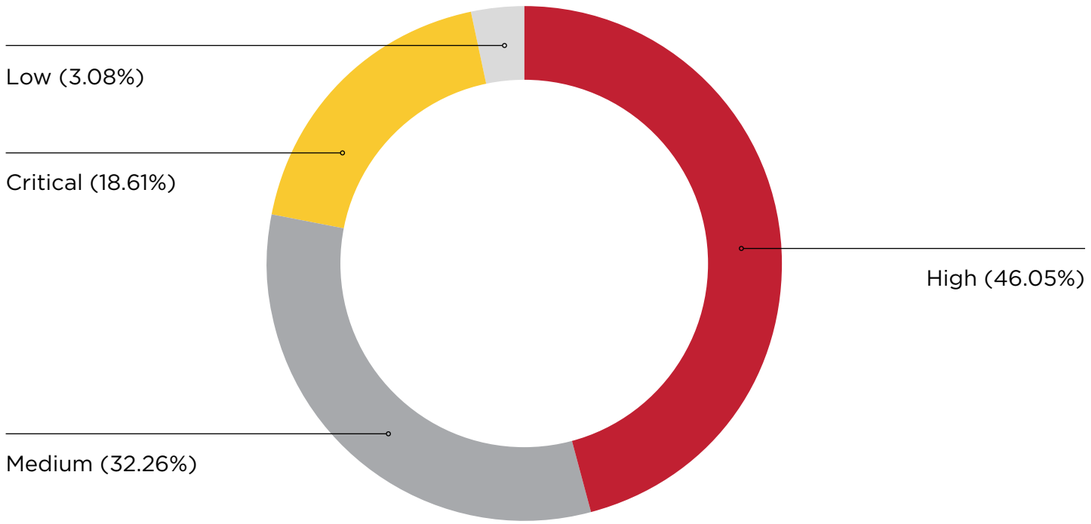
How Many Vulns, and How Critical?

During 1H 2022, 747 XIoT vulnerabilities were published affecting 86 vendors across industrial, healthcare, and commercial technology vendors.

The vast majority of XIoT vulnerabilities have CVSS scores that are either critical (19%) or high severity (46%).

While the number of published vulnerabilities is relatively flat from the last Team82 report, there are, on average, still 125 vulnerabilities a month that are being published and addressed across sectors making up the XIoT.

Team82 disclosed 44 vulnerabilities affecting 11 vendors, bringing its total number of disclosed vulnerabilities to 335.



Let's Talk About Firmware

In past reports, Team82 has discussed the relevant challenges in updating firmware within industrial domains, as well within embedded systems, medical devices, and other domains. Fewer remediations traditionally are made available to address firmware vulnerabilities. Firmware update cycles are longer, and when they're updated, network devices are generally addressed more frequently than IoT devices or those at the Basic Control level of the Purdue Model for ICS.

Vendors prioritize patching software over firmware because update cycles are quicker, and operators can take advantage of regular maintenance windows to install software patches, in particular for critical applications.

In 1H 2022, we've seen a bit of a reversal of that trend where published firmware vulnerabilities are almost on par with software vulnerabilities, unlike the 2H 2021 report when there was almost a 2-to-1 disparity between software vulnerabilities and firmware bugs.

Even better news may be found in the total number of fully remediated firmware vulnerabilities in the 1H 2022 dataset. We see significant growth from the last report with 233 firmware flaws fully remediated by vendors, and another 69 where partial remediation was provided.

SOFTWARE

FIRMWARE

1H 2022

40%

Fully or partially remediated firmware vulnerabilities

2H 2021

21%

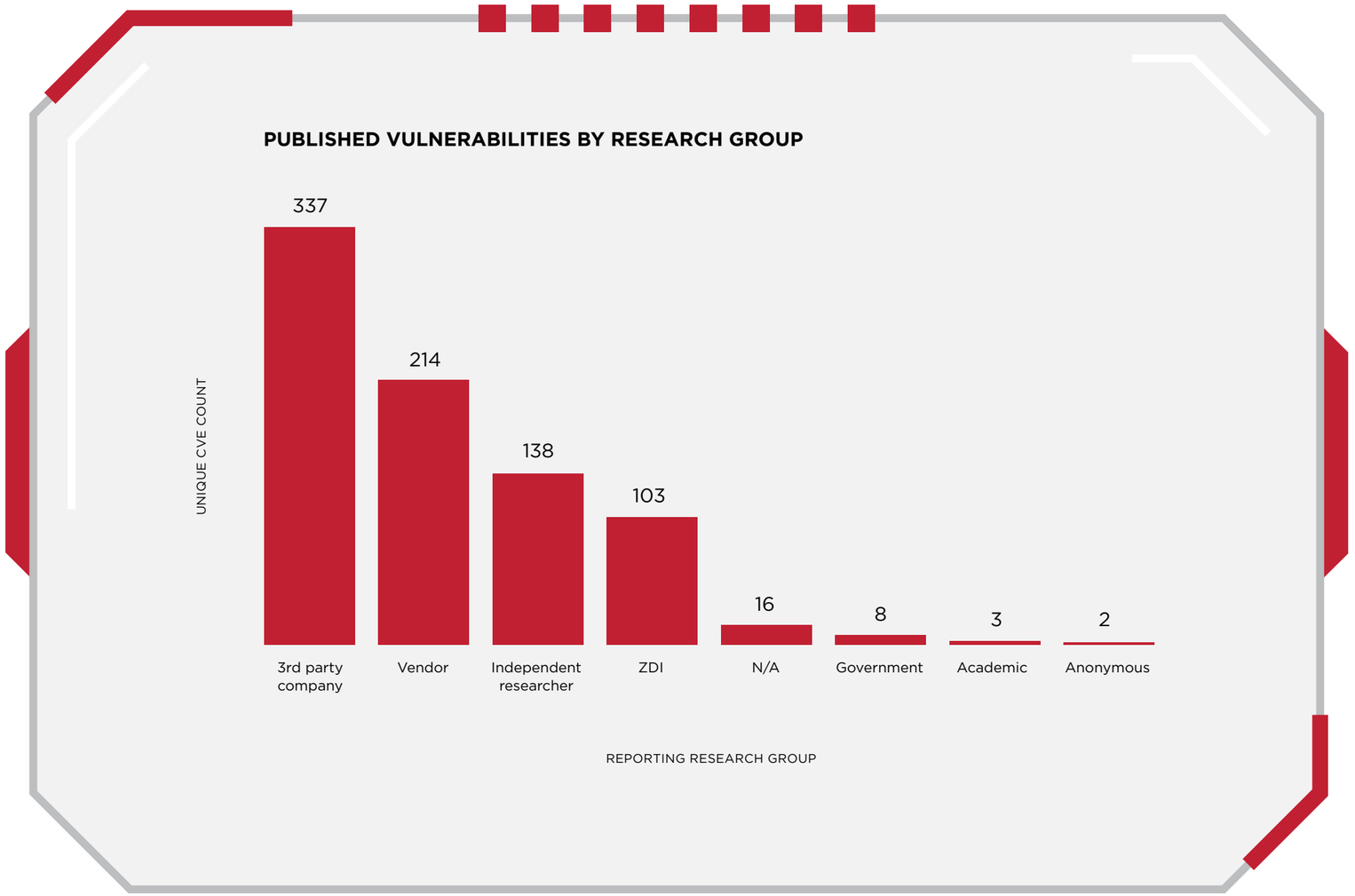
Fully or partially remediated firmware vulnerabilities

Eyes on Vendor Self-Disclosures

For the first time, vendor self-disclosures have surpassed independent research outfits as the second most prolific vulnerability reporters. Vendors accounted for 214 published CVEs in 1H 2022, trailing only third-party security companies, which reported 337. The 214 published CVEs almost doubles the total in Team82's 2H 2021 report of 127.

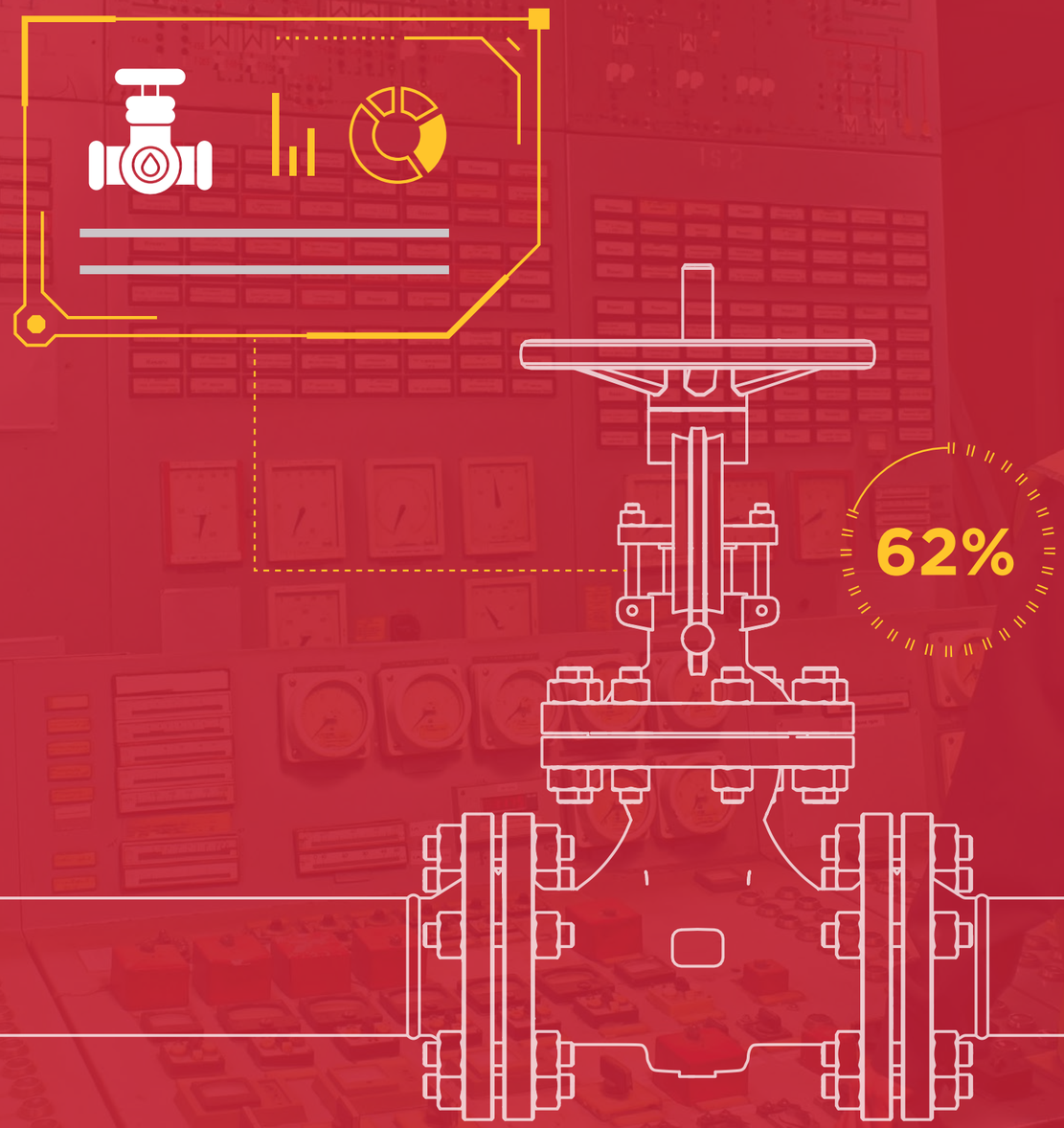
For years, Team82 has been vigilant not only about finding vulnerabilities in industrial and IoT software and firmware, but also about ensuring a safer ecosystem. That vigilance includes improving coordinated disclosures with vendors, and helping smaller, less-resourced organizations with establishing the basics for a vulnerability disclosure program.

Vendor product security and safety teams have sprung up with more frequency, and the numbers in Team82's dataset for the 1H 2022 are starting to bear this out, as you'll see in the "Origin of XIoT Vulnerabilities" section of this report.



TEAM82

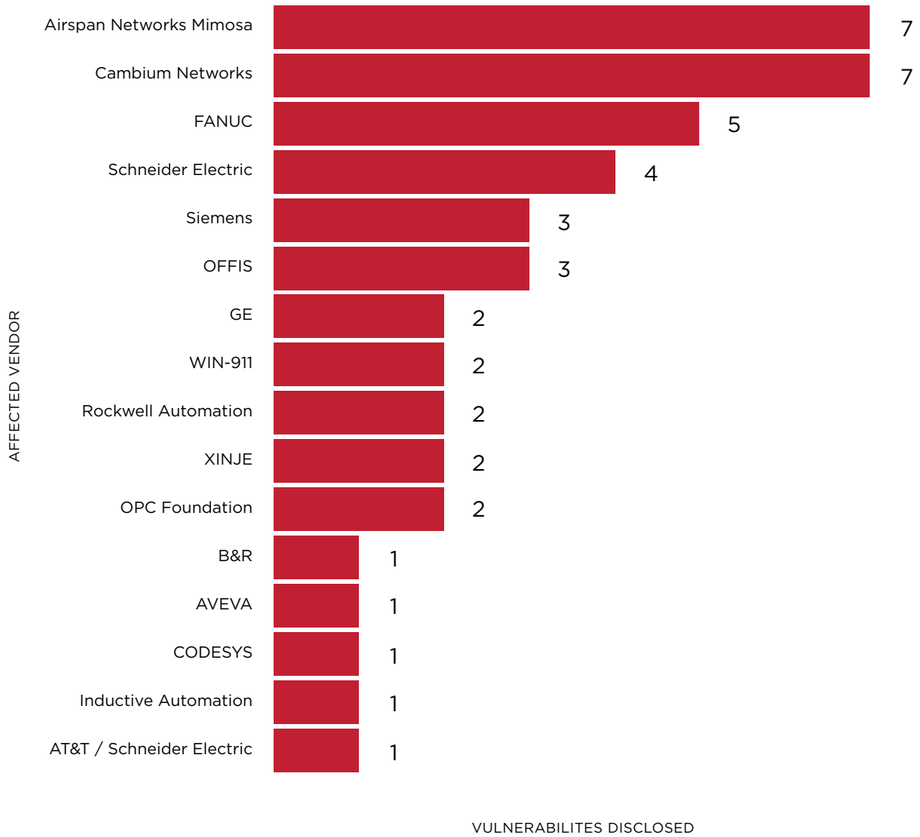
Assessment of 1H 2022 Disclosures



ASSESSMENT OF XIOT VULNERABILITIES DISCLOSED BY TEAM82 1H 2022

Team82's diligent work to secure the XIoT ecosystem is showing distinct benefits that will be illustrated throughout this report. In the first six months of this year, Team82 disclosed more than 40 OT, enterprise IoT, and medical device/protocol vulnerabilities affecting 16 technology vendors.

While automation vendors still dominate the vulnerability disclosures in Team82's dataset, more enterprise IoT and vendors in the healthcare space emerged.



DISCLOSURE NUMBERS

335
Vulnerabilities disclosed since 2018

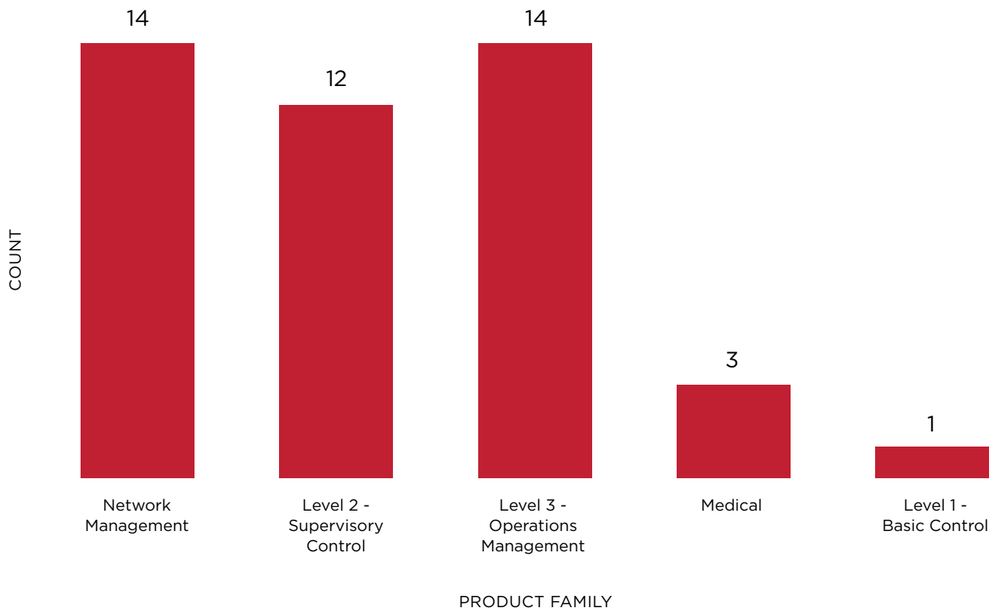
56
Affected Vendors

11
Vendors who initiated vulnerability disclosure programs after a Team82 disclosure

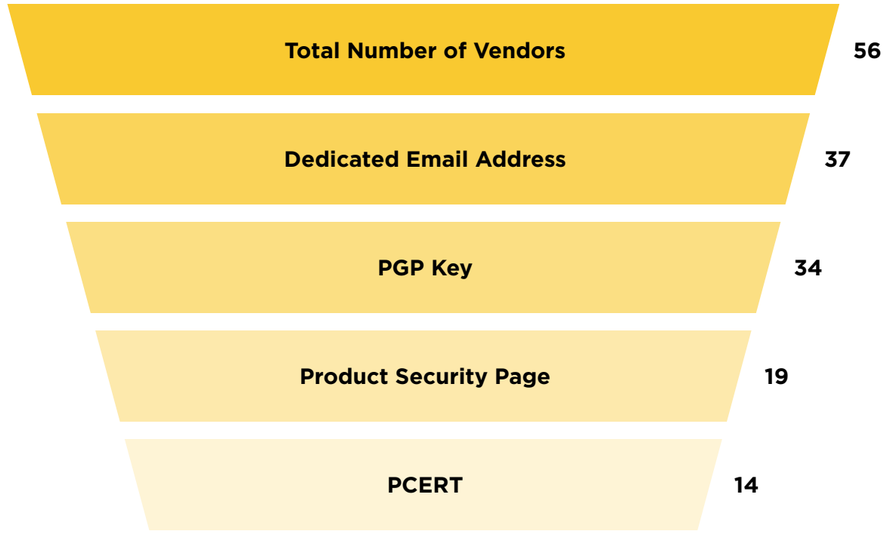
44
Vulnerabilities disclosed in 1H 2022

Breaking down Team82's 44 1H 2022 vulnerability disclosures, network management and Purdue Model Level 3 devices (historians, engineering workstations) domainate.

TARGETED PRODUCT FAMILY



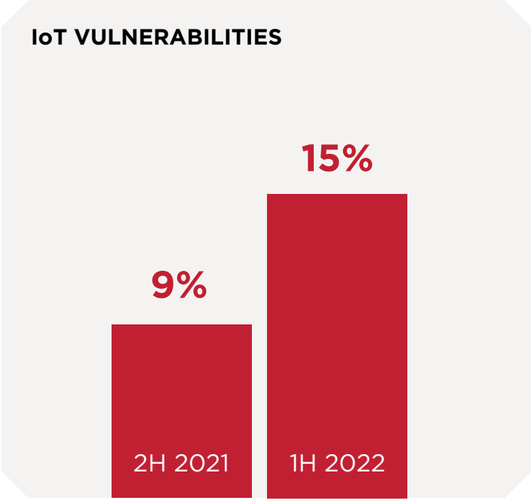
The bigger win may be in the growing maturity of vendors' vulnerability disclosure programs with whom Team82 has coordinated disclosures. Team82 is interacting with more vendors who have established product emergency response teams, have dedicated webpages on their sites to product security that include email addresses for vulnerability reporting, and have made available a public PGP key for secure exchange of sensitive information about security flaws. We wrote more about this here: "Understanding and Improving the XIoT Vulnerability Disclosure and Publishing Process."



XIoT VULNERABILITIES ASSESSMENT

ASSESSMENT OF XIOT VULNERABILITIES DISCLOSED IN 1H 2022

The number of published vulnerabilities in Team82's XIoT current dataset is relatively flat from its 2H 2021 report, while the number of affected vendors rose slightly to 86. What's notable is the growth in reported enterprise IoT vulnerabilities from 9% to close to 15%.



Commercial systems, including building automation systems, surveillance systems including security cameras, alarms, and door locks are increasingly being connected and managed online. It's crucial to understand that every enterprise, regardless of industry or core competence, has some measure of OT and IoT connected to its network.

It's here where cyber-physical systems that sustain our ability to innovate, have a direct impact on our way of life. Vulnerability management of connected systems is paramount because any disruption may impact physical safety and security as well as our economic prosperity.

DISCLOSURE BY THE NUMBERS

747

Published XIoT vulnerabilities in 1H 2022

86

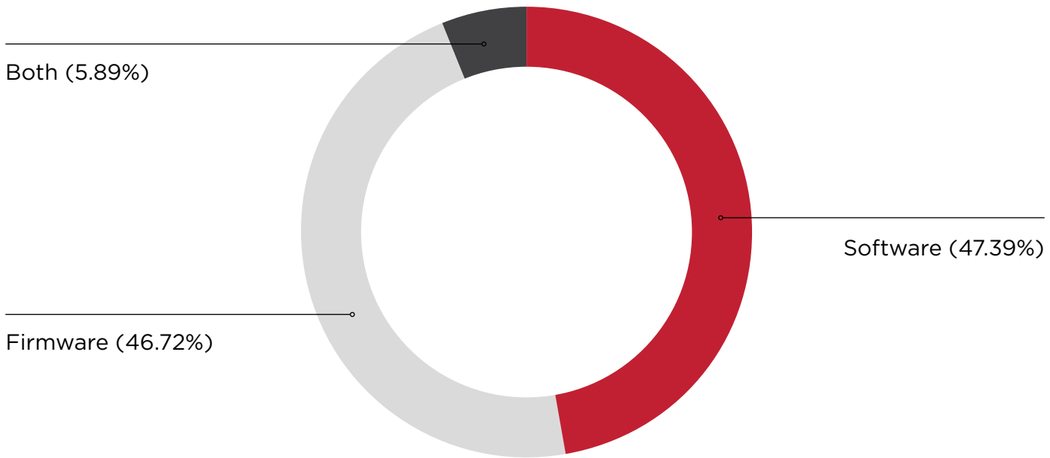
Affected Vendors

Affected XIoT Components: The Software/Firmware Story

Vulnerability disclosures largely affect either software or firmware; there are some cases in which a vulnerability affects several components that may impact both software and firmware. In the past, disclosures of software vulnerabilities have dwarfed firmware, indicating a prevalence of researchers examining software for bugs, and the relative challenges in researching and patching firmware. Software updates, for example, are often prioritized over firmware given the comparative ease to test and distribute software patches.

We've seen a dramatic rearrangement of the deck chairs in this category from Team82's 2H 2021 report when 62% of vulnerabilities were software-based, and 37% were firmware-based.

1H 2022 disclosures of software-based vulnerabilities were nearly matched by vulnerabilities in firmware.



Key Event: Industroyer2

Throughout the State of XIoT Security Report, Team82 will highlight some of the key events that shaped the 1H 2022.

Russia's invasion of Ukraine on Feb. 24 ignited fears of cyberattacks accompanying the kinetic fighting in the streets and skies of Ukraine. Electric grids within Ukraine were perceived as targets, as were other critical cyber-physical systems integral to the way of life inside the war-torn country.

In April, security vendor ESET reported that a variant of the 2016 Industroyer malware used by the Sandworm APT against portions of Ukraine's power grid was deployed inside a Ukrainian electricity provider. The malware was contained before it was triggered, officials said.

The variant, named Industroyer2, was purpose-built to target industrial equipment communicating over IEC-104 (IEC 60870-5-104), in this case power-system automation applications used in high voltage electrical substations. ESET and CERT-UA said the variant was built using the same source code as the original Industroyer, also known as CrashOverride.

Industroyer2 is capable of communicating with multiple ICS devices simultaneously, an analysis exposed several configuration values including the ASDU address, IOA, timeouts, and more. The malware terminates legitimate processes and renames applications in order to prevent automatic restarts of the targeted processes. Its purpose was to disconnect power to people in the country served by this plant.

Affected Product Families

Vulnerabilities in IoT devices have climbed since Team82's 2H 2021 report, trailing only Operations Management and Basic Control OT devices.

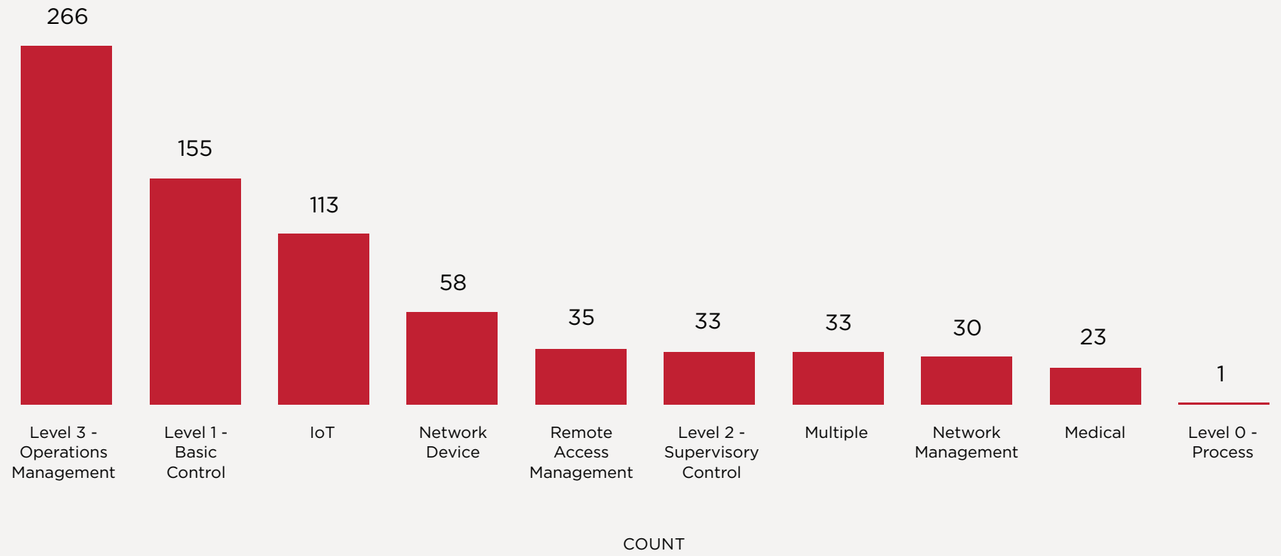
As in the last Team82 report, most of the published vulnerabilities affect devices at the Operations Management (Level 3) level of the Purdue Model, such as Historian or OPC servers; these are also largely software-based vulnerabilities.

About 25% of disclosed vulnerabilities affect the Basic Control (Level 1) and Supervisory Control (Level 2) levels of the Purdue Model. Exploits at this level are often firmware-based and can allow an attacker to reach lower levels and affect the process itself, making them an attractive target.

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.

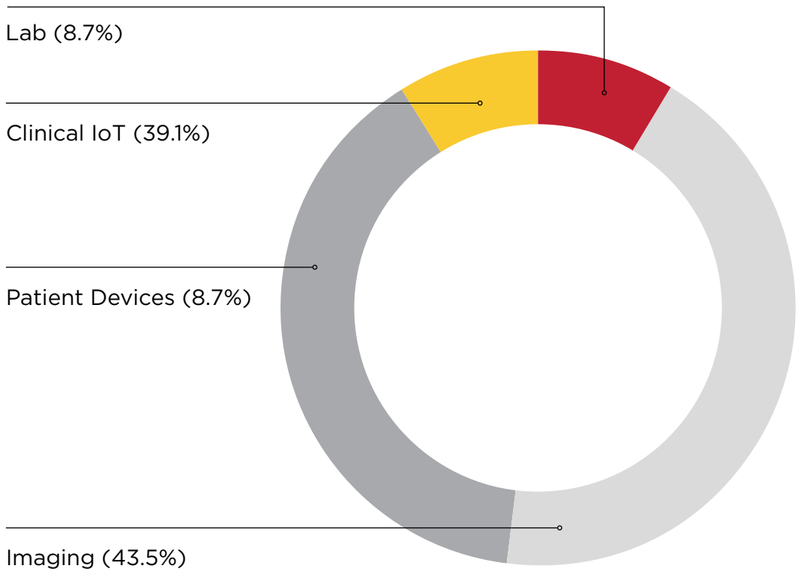
Vulnerabilities in connected medical devices, known as the internet of medical things (IoMT), meanwhile, have surfaced in Team82's dataset, primarily among imaging systems and the protocols that support them, such as the DICOM communication standard.

AFFECTED PRODUCT FAMILIES

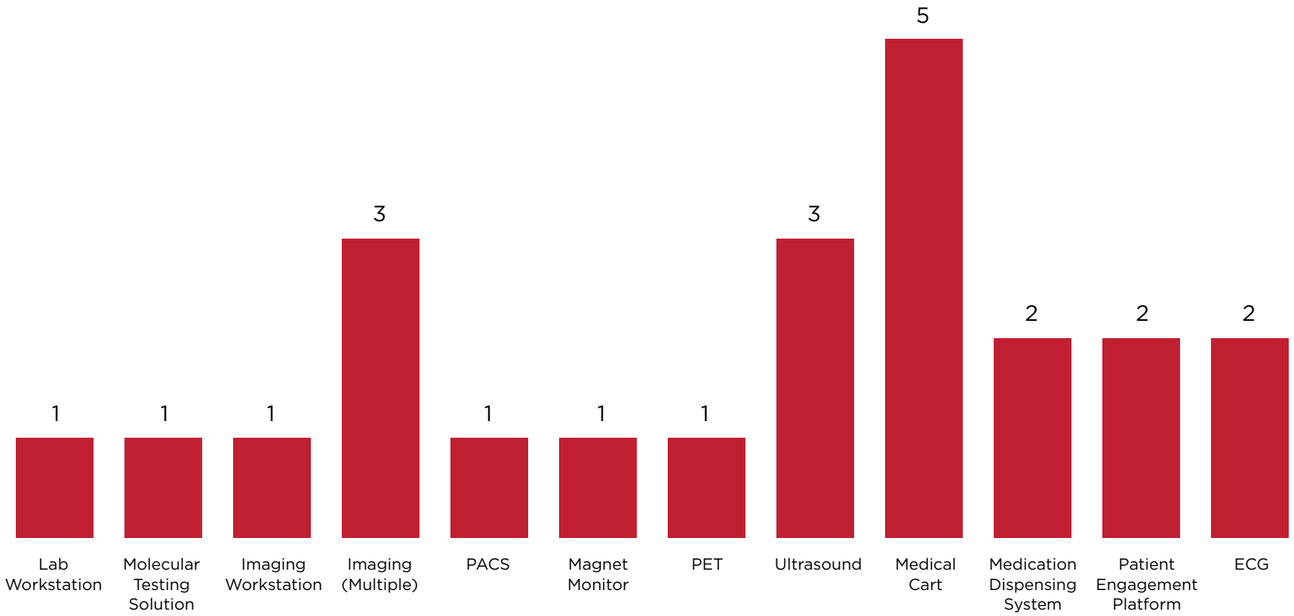


Multiple flaws in clinical IoT devices—such as medical carts, dispensing systems and patient engagement applications—also were published in the 1H 2022, as were security issues found in patient devices and clinical lab tools.

VULNERABILITIES BY MEDICAL CATEGORY



VULNERABILITY BY PRODUCT TYPE

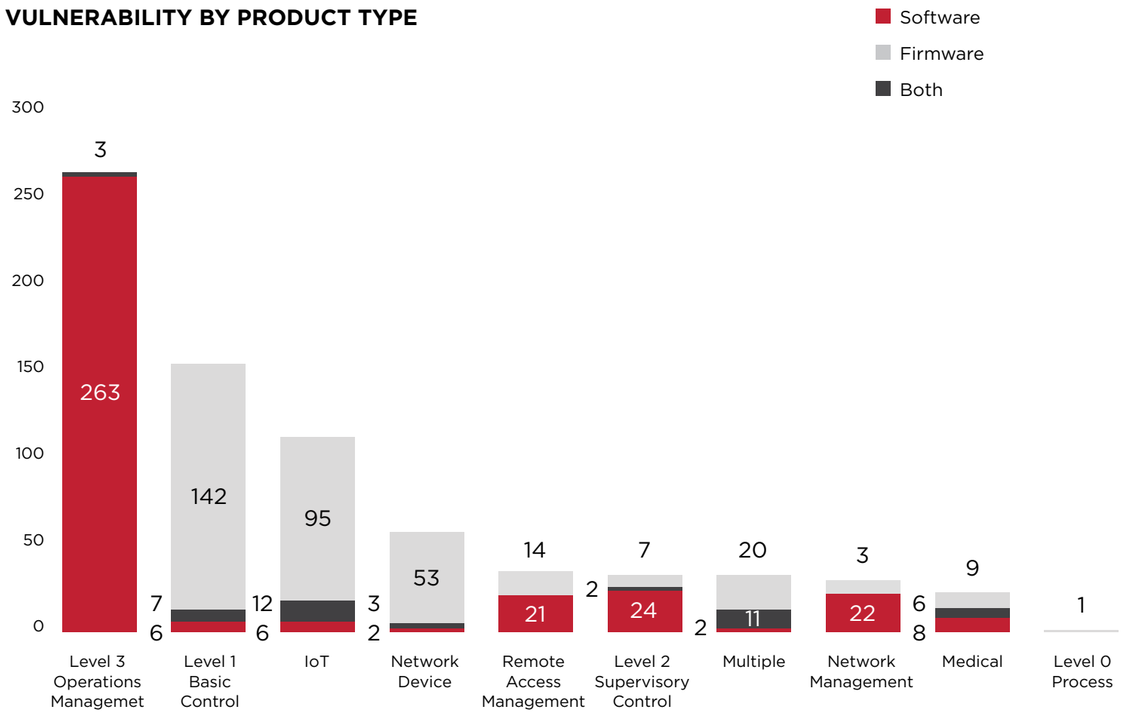


COUNT OF VULN BY PRODUCT TYPE

Firmware/Software Division in Product Families

The division of firmware and software vulnerabilities within product families—especially in IoT and field devices—could be quite interesting. 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 consider the product types affected by it. Some examples could be vulnerable software configurations running on HMIs, or an ethernet module connected to a pump.

VULNERABILITY BY PRODUCT TYPE



Key Event: Incontroller/Pipedream

Security firm Mandiant reported on a suite of ICS attack tools it called Incontroller (aka Pipedream). Such tools are a rarity, and immediately, comparisons were made between Incontroller and Triton, a tool built to disable safety systems crucial to industrial operations.

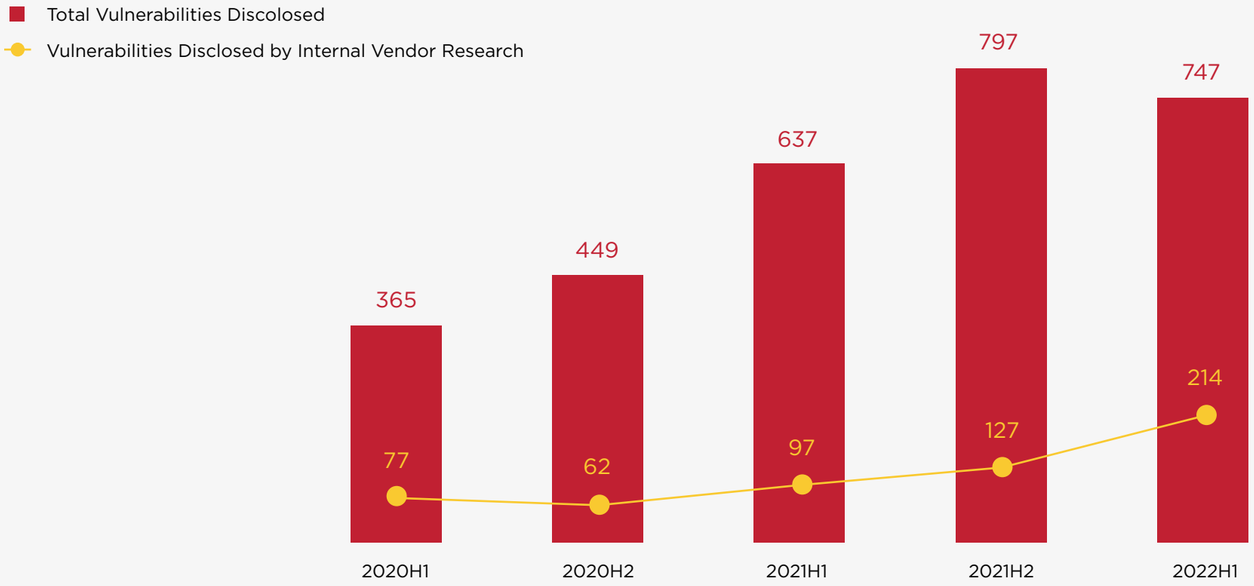
Incontroller's flexibility was concerning to researchers who quickly analyzed that its three components could impact critical infrastructure anywhere in the world, disrupt service delivery, and sow chaos among affected populations.

Incontroller has three tailor-made components: Tagrun, Codecall, and Omshell, that target OPC UA servers, various Schneider Electric PLCs, and Omron PLCs respectively. These components were built only after extensive reconnaissance of target environments, Mandiant said. Each component was made to interact with specific industrial equipment and interfere with critical processes through sophisticated means reserved previously for the Stuxnets, Tritons, and Industroyers of the world.

Origin of XIoT Vulnerability Discoveries

As we mentioned in the Team82 section of this report, more OT, IoT, IoMT vendors are establishing vulnerability disclosure programs than ever before. Companies are formalizing a means of accepting vulnerability reports from research teams such as Team82, dedicating resources to triaging bug reports, improving relationships and communications with research teams, and closing the windows of exposure for users from when bugs are discovered and reported to when a fix or mitigation is made available.

VENDOR SELF-DISCLOSURE TRENDS



70%

In our 1H 2022 dataset, the vast majority of vulnerability disclosures came from sources external to the affected vendor.

28%

This figure is a dramatic leap from Team82's 2H 2021 report when 16% of vulnerability disclosures came from internal vendor research teams. That number has nearly doubled to 28% in the first six months of 2022.

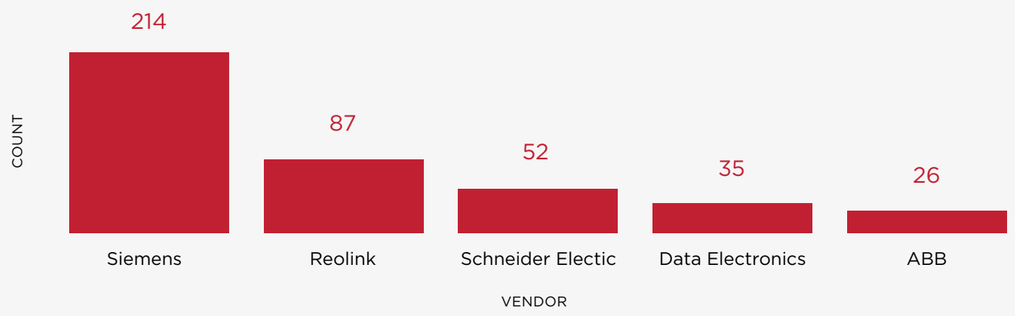
Affected XIoT Vendors

The number of affected vendors grew by four from the 2H 2021 report, and is on track to surpass 2021's total of affected vendors. Team82 attributes a number of factors to this; it's important to understand that XIoT vulnerability research continues to grow and mature as vendors handle vulnerabilities in products never designed to be connected to the internet.

Market-leading vendors such as Siemens and ABB are in the top five of the most affected vendors. These automation companies build products across the XIoT spectrum, and in tandem, have established product security teams that work closely with external researchers to find and fix every vulnerability. Team82 has forged research partnerships with many of these vendors as well as others who are nurturing newly minted internal security and response teams, contributing to a largely more secure ecosystem.

Noteworthy is the ascension of Reolink to No. 2 on the list of affected vendors. Reolink is a vendor of connected security and surveillance cameras, one of the most affected product families with published vulnerabilities in the 1H of 2022.

VULNERABILITIES PER VENDOR TOP 5



In the current Team82 dataset, Siemens is the vendor affected by the most reported vulnerabilities, many of which were discovered by the internal Siemens Product CERT.

86
Affected Vendors

147
2021 Total Affected Vendors

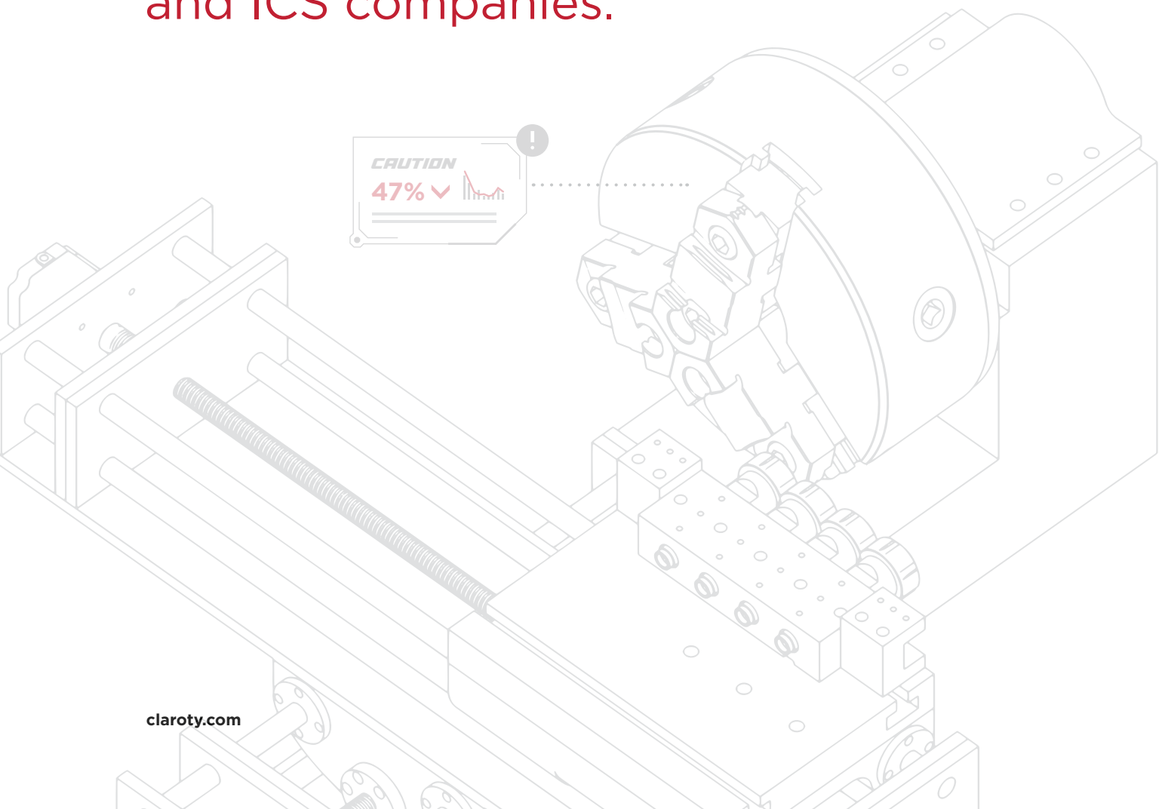
We should point out that a significant number of disclosed vulnerabilities for any one vendor is not a reflection of its product security or ability to scrutinize for vulnerabilities.

The opposite is likely true

- Market-leading vendors allocate ample resources to product security
- Our numbers indicate they're finding more vulnerabilities than ever before
- The age, catalog, and install base of each vendor influences the number of disclosed vulnerabilities affecting products.

Vendors with First-Time Vulnerability Disclosures in 1H 2022

19 XIoT vendors experienced first-time published disclosures in the 1H 2022; the list is a mix of medical device makers, building automation vendors, IT, OT, and ICS companies.



VENDORS	PRIMARY INDUSTRY
Aethon (owned by ST Engineering)	Healthcare
Mimosa Networks (Airspan Networks)	IT Technology
Automated Logic	Building Automation
Cambium Networks	IT Technology
LenelS2	IoT
Elcomplus	IT
Exemys	IT
Fernhill Software	Automation
Illumina	Healthcare
Keysight Technologies	Manufacturing
LifePoint Informatics	Healthcare
Meridian Cooperative	Utility software
OFFIS	Healthcare
PTC	Industrial IoT
Pyramid Solutions	Automation
Ricon Mobile	IoT
Sécheron	Manufacturing
XINJE	Automation
Valmet	Automation

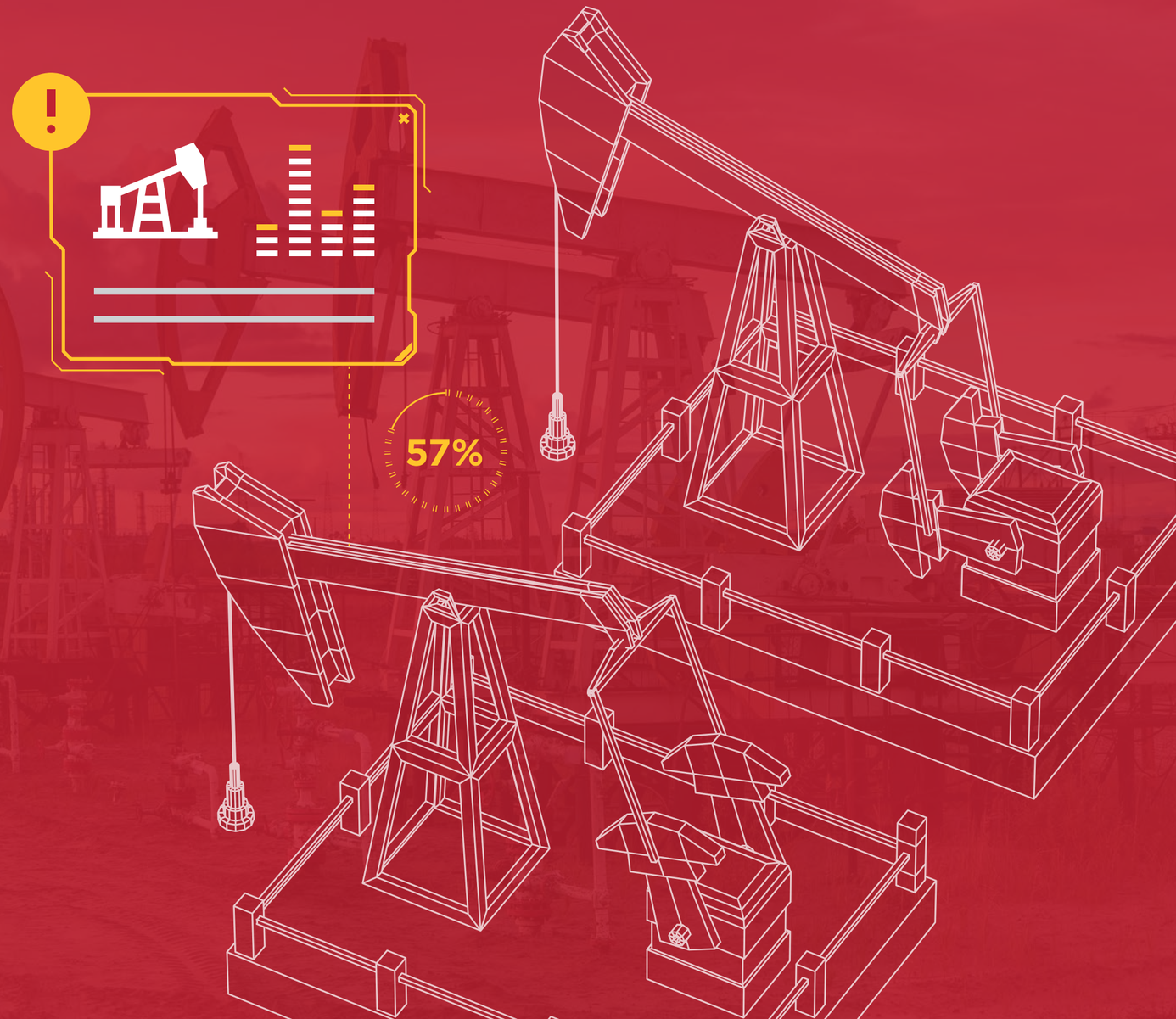
MITIGATIONS/ REMEDIATION

Mitigations

Remediations

End-of-Life Products

Key Event: OT:ICEFALL



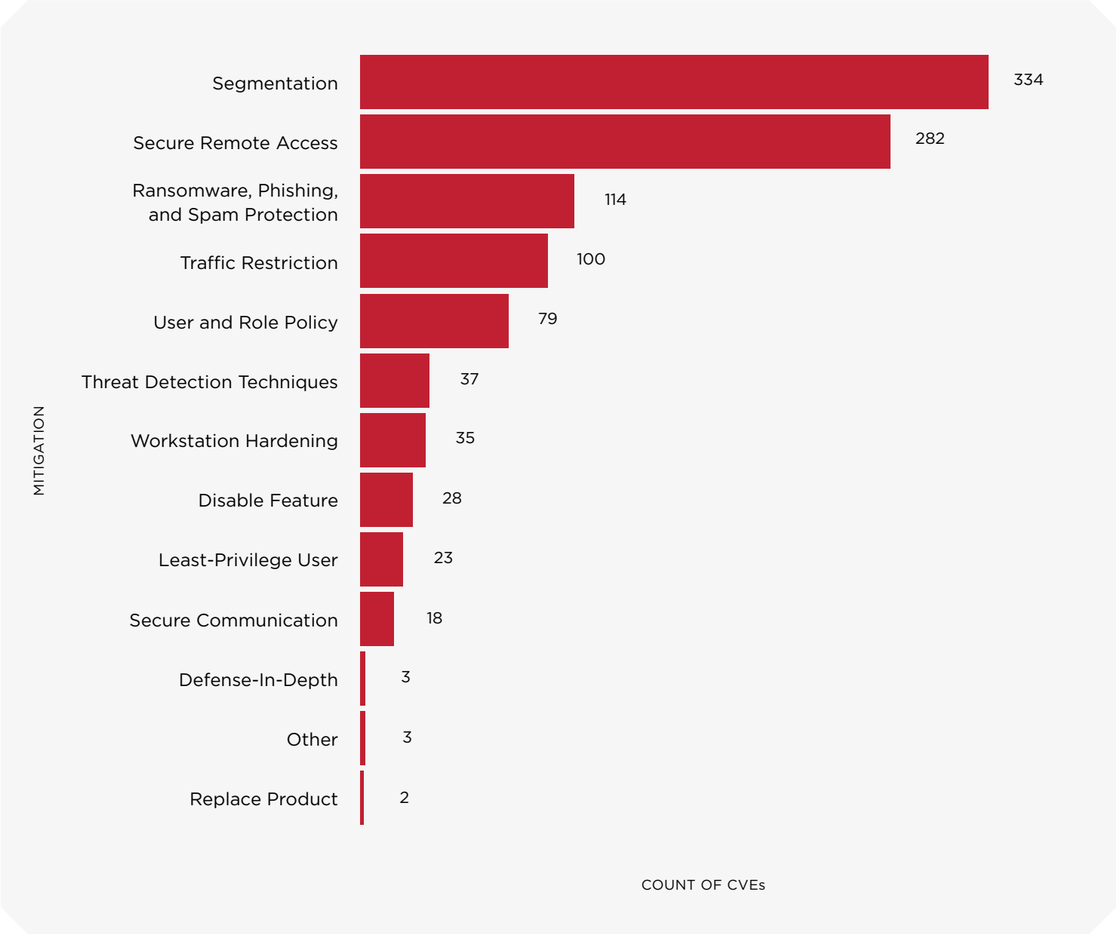
MITIGATIONS/REMEDIATION

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, right. For example, network segmentation is the top step, and should be a top consideration for defenders ahead of other options on our list, including basic security hygiene such as ransomware awareness (phishing mitigations), traffic restriction, user- and role-based policies, and the principle of least privilege.



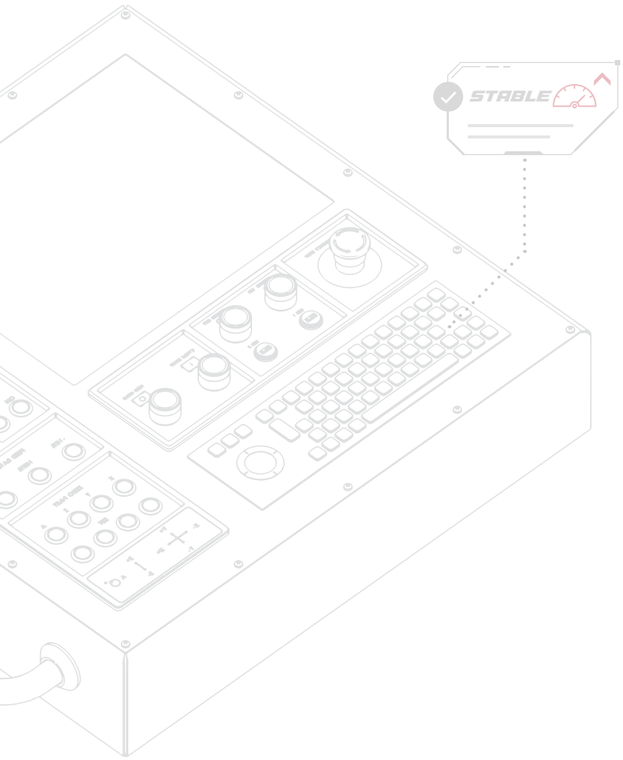
Network segmentation is an important control as air-gaps become a relic of the past and perimeters erode as enterprises move data, applications, infrastructure and services to the cloud.

Segmentation would likely involve virtual zoning that allows for zone-specific policies that are tailored to engineering and other process-oriented functions, or alternatively separating between the public space and PHI servers in medical facilities.

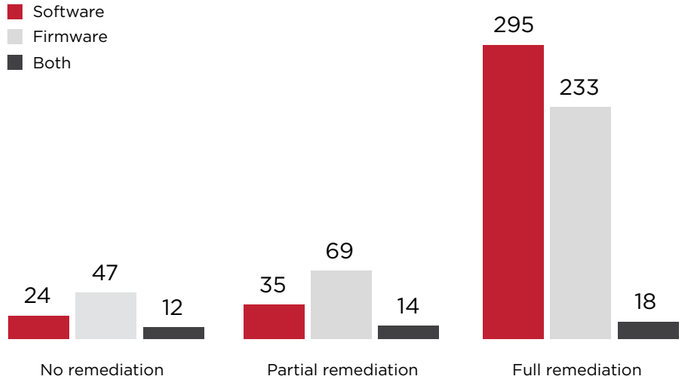
Segmentation goes hand-in-hand with secure remote access, the second most recommended mitigation. Secure remote access involves not only separating critical zones from the rest of the IT and OT networks, but also securing remote sessions through the addition of encryption, authentication, and authorization capabilities.

Remediations

The disparity between software- and firmware-based vulnerabilities is apparent here as well, as the number of full remediation options for firmware flaws has significantly grown since Team82's 2H 2021 report.



REMEDIATION BY FIRMWARE/SOFTWARE 1H 2022



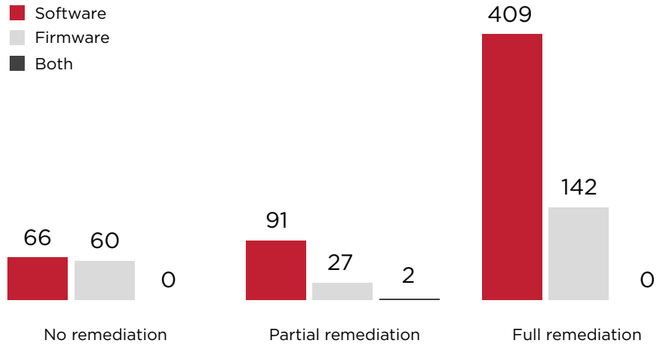
54%

of full remediated vulnerabilities are software based. Emphasizing the ease of patching software over firmware.

62%

of partially or not remediated vulnerabilities when exploited, could result in remote code execution or in denial-of-service

REMEDIATION BY FIRMWARE/SOFTWARE 2H 2021



74%

of full 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 not remediated vulnerabilities when exploited, could result in remote code execution or in denial-of-service

REMEDIATION BY THE NUMBERS

71%

Full remediation: All products are patched and updated

20%

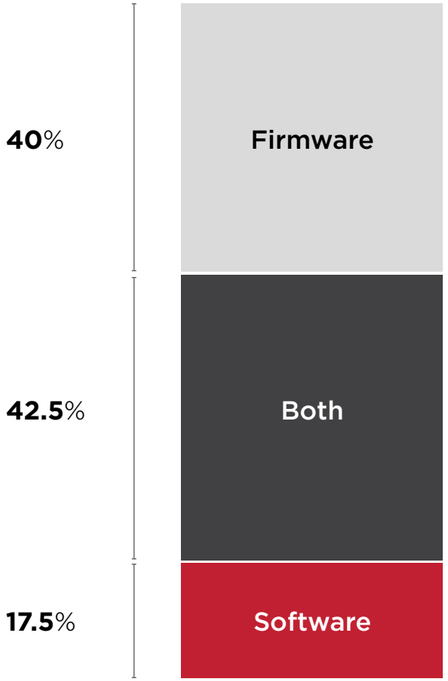
Partial remediation: Not all affected products have a fix

9%

No remediation: Product remains unpatched, and without mitigations

End-of-Life Products

40 vulnerabilities affect end-of-life products that are no longer supported by the vendor.



Key Event: OT:ICEFALL

Security vendor Forescout and CISA disclosed to industries the discovery of 56 vulnerabilities in operational technology products sold by 10 vendors. Largely, the vulnerabilities were rooted in insecure design practices, and marred by weak cryptography, broken authentication, insecure firmware updates, and flaws that enabled remote code execution on ICS devices.

Dubbed OT:ICEFALL, the disclosed vulnerabilities were a stark warning that cyber-physical systems security still lags, and given the increased connectivity to critical applications and systems, the situation is close to intolerable.

A familiar refrain hovers over the OT:ICEFALL disclosure in that many of these critical devices were never developed with today's connectivity in mind. Proprietary protocols add to the design and remediation complexity surrounding OT:ICEFALL. Lastly, as Forescout points out, an advanced attacker has a distinct advantage over defenders and needs only a relatively short number of months to reverse engineer these protocols, find exploitable vulnerabilities, develop and deploy exploits against a target.

END-OF-LIFE EXPLOITABILITY

78%

of published vulnerabilities affecting end of life are exploitable via a network attack vector

65%

of published vulnerabilities allow an attacker to carry out remote code execution or denial-of-service attacks

15%

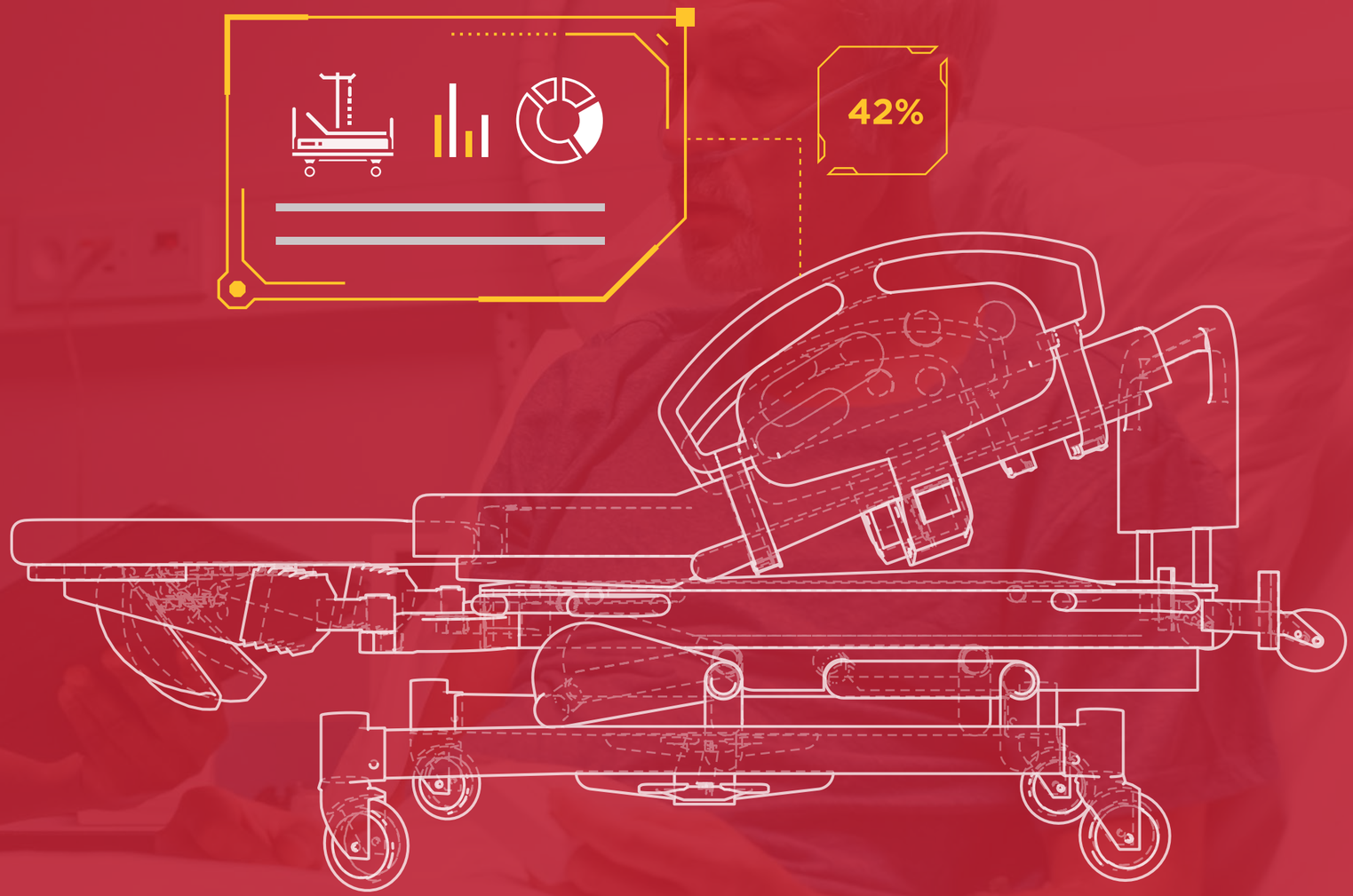
of published vulnerabilities in end-of-life products affect Level 1 devices on the Purdue Model for ICS

IMPACT

Attack Vector Distribution

Availability

Key Event: Healthcare and Ransomware



Impact

Users largely rely on two frameworks when prioritizing vulnerability remediation:

CVSS: The Common Vulnerability Scoring System is a scoring framework used to illustrate the severity and characteristics of vulnerabilities.

CWE: The Common Weakness Enumeration is a specification used to describe the cause of software and firmware vulnerabilities.

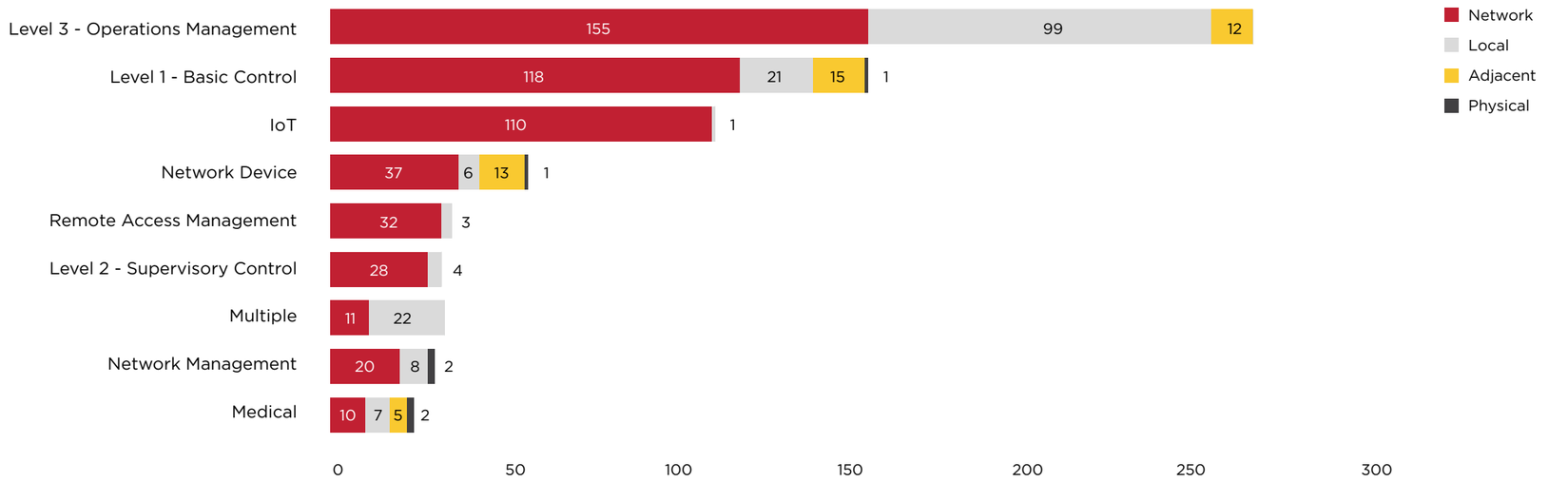
Attack Vector Distribution

XIoT vulnerabilities can be targeted remotely over the network, locally with physical access to devices or networked components, and adjacently by an attacker with a foothold on a local area network that's not on the same network segment as the targeted device.

Attacks over the local attack vector dropped from 31% in Team82's 2H 2021 report, while attacks over the network climbed 7%. Local attacks may require some sort of user interaction to exploit vulnerabilities, right.

These attacks would include social engineering tactics such as phishing or spam to enable an attacker gaining an initial foothold on the network. Awareness and protection against these tactics is critical.

During the 1H 2022, the network attack vector is dominant in all product family categories.



ATTACK VECTOR DISTRIBUTION

70%
Over the network

24%
Local access

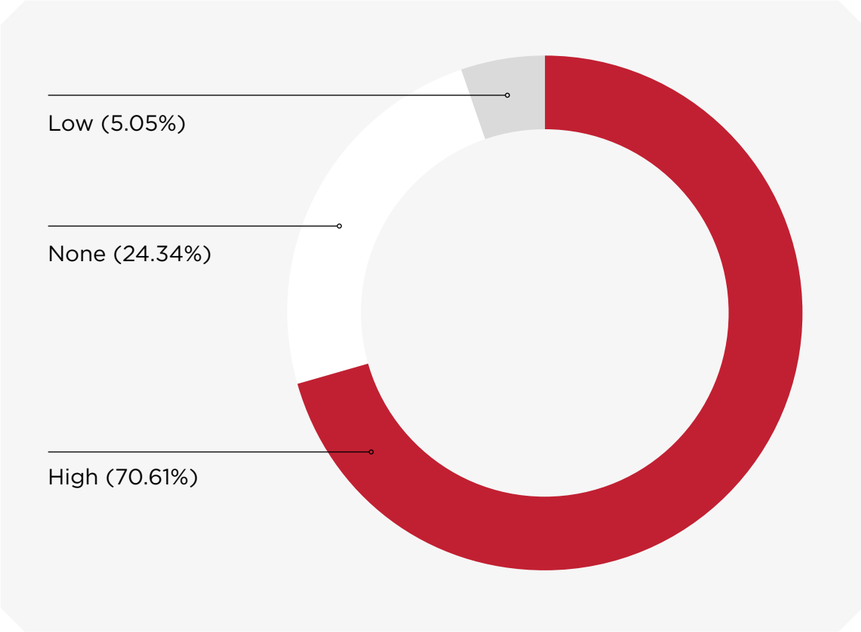
6%
Adjacent

62%
Percentage of vulnerabilities exploited via a local attack vector and require user interaction.

Availability

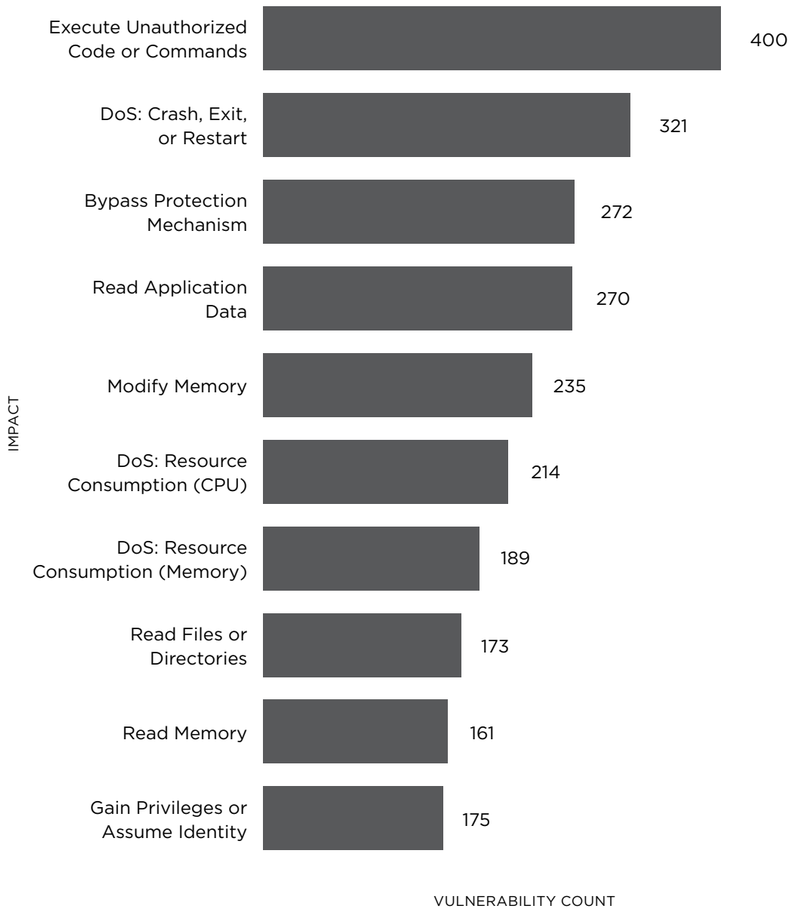
Availability is the impact metric most applicable to XIoT device vulnerabilities. Though technically relevant to any type of network, the CIA triad that includes confidentiality and integrity does not always encompass what are arguably the two most important risk variables for XIoT: reliability, and safety.

Close to three-quarters of vulnerabilities in Team82's 1H 2022 dataset have a high impact on system and device availability.



The list, right, further illustrates the potential impact to availability, reliability, and safety of XIoT systems posed by vulnerabilities in the 1H 2022 Team82 dataset.

VULNERABILITY COUNT BY IMPACT TOP 10



The top five most prevalent CWEs from Team82's dataset are also prominent on MITRE Corp.'s 2022 CWE Top 25 Most Dangerous Software Errors list. These vulnerabilities can be relatively simple to exploit and enable adversaries to disrupt system availability and service delivery.

1. **CWE-20 : Improper Input Validation (12.34%) No. 4 on the 2022 CWE Top 25**
2. **CWE-787: Out-of-bounds Write (6.68%) No. 1 on the 2022 CWE Top 25**
3. **CWE-79: Improper Neutralization of Input During Web Page Generation (Cross-site Scripting) (5.4%) No. 2 on the 2022 CWE Top 25**
4. **CWE-89: Improper Neutralization of Special Elements used in an SQL Command (SQL Injection) (4.5%) No. 3 on the 2022 CWE Top 25**
5. **CWE-798: Use of Hard-coded Credentials (3.21%) No. 15 on the 2022 CWE Top 25**

Simple coding errors such as input validation, buffer-related memory vulnerabilities, and SQL injection continue to plague software development, and are reflected prominently in Team82's dataset and the MITRE list.

Key Event: Healthcare and Ransomware

Ransomware and extortion attacks continue to plague healthcare systems. Baptist Health System of Texas reported in June that it was victimized by ransomware last December and that the attack was cover for an extensive data breach that spilled patient contact information and insurance data.

Yuma Regional Medical Center of Arizona also announced in June it was victimized in an April ransomware attack that also resulted in the loss of more than 700,000 patient records. Shortly after this incident, the U.S. Department of Health and Human Services reported that healthcare breaches had doubled from the same period in 2021. Between Jan. 1 and May 31, HHS listed 244 electronic data breaches of healthcare organizations with at least 500 victims on its site. The figure for that same range in 2021 was 137.

Attackers target industries such as healthcare because of their high availability requirements; any impact to patient health makes such a victim more likely to pay a hefty ransom in order to reestablish access to patient records and services, and avoid consequences to patient care such as misdiagnosis or incorrect therapy.

Basic security hygiene, meanwhile, is crucial to keeping ransomware at bay.

- Adhere to the principle of least privilege; limit admin accounts
- Beware of untrusted sources sending emails and attachments
- Users should not supply credentials, personal, financial or company information
- Backup important files and store them in a secure location or elsewhere on the network
- Keep operating system and key application patches up to date
- Report phishing and suspicious emails to security or IT staff

RECOMMENDATIONS

Network Segmentation

Secure Remote Access

Managing Risk from the Cloud

RECOMMENDATIONS

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

Network Segmentation

Segmentation is far and away the champion of XIoT mitigation recommendations. Within OT networks, segmentation has been a security fixture as operators use it to limit external—and internal—access to critical systems and resources.

Air-gapped networks have been the de facto security practice to keep field devices and management systems clear of external connections. However, it's rapidly losing favor as OT, medical devices, and embedded systems running IoT devices are connected to the internet and managed via the cloud.

Users are urged to virtually segment assets, and prioritize segmentation:

- Segment networks virtually and configure them 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, Medical and IoT specific protocols in order to detect and defend against anomalous behaviors.

RECOMMENDATIONS

Secure Remote Access

Remote administration of XIoT devices is commonplace for internal security analysts and network managers, as well as for third-party contractors and vendors. Strategically, organizations must carefully manage privileges to medical devices, industrial control systems—in particular, field devices and systems at management levels of the Purdue Model for ICS—and other XIoT systems.

Secure remote access that streamlines access to internal employees and third parties, extends a zero-trust approach to privileges, and offers auditing and response capabilities is a must to reduce mean-time-to-repair.

Security practitioners are encouraged to do the following:

- Use a zero-trust implementation to help reduce downtime, ensure availability and service delivery.
- Verify VPN versions are patched and up to current versions
- Monitor remote connections, particularly those to OT networks, ICS devices, critical medical equipment, e-PHI servers and critical IoT devices.
- Enforce granular user-access permissions and administrative controls following the principle of least privilege.

RECOMMENDATIONS

Manage Risk from the Cloud

Process efficiency is a dominant business reason to connect XIoT devices and systems to the internet and manage them from the cloud. Doing so brings enhanced analytics that improve operational efficiency and usability; it also carries risk that must be managed.

Many XIoT devices, especially those within OT, are no longer air-gapped and therefore have a much larger attack surface. Threat actors may see an opportunity to target vulnerabilities exposed by connectivity at scale.

Risk management in cloud managed OT networks can be broken down into several security aspects, right, security practitioners and ICS companies should do the following:

Data Security: Encryption and Secure Communication

- Verify XIoT devices' cloud support protocols, such as MQTT or HTTPS via Web Client/ REST. Within OT, for example, these are used to exchange data between PLCs and the cloud.
- Use security mechanisms, such as encryption and signing of data and communication with X.509 certificates or hardware-based encryption.

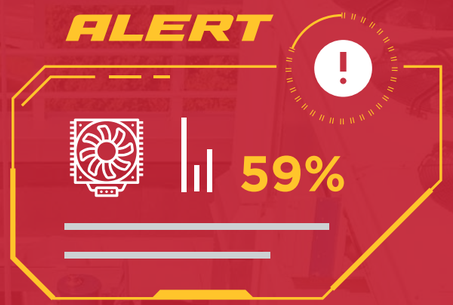
Authentication and Identity Management

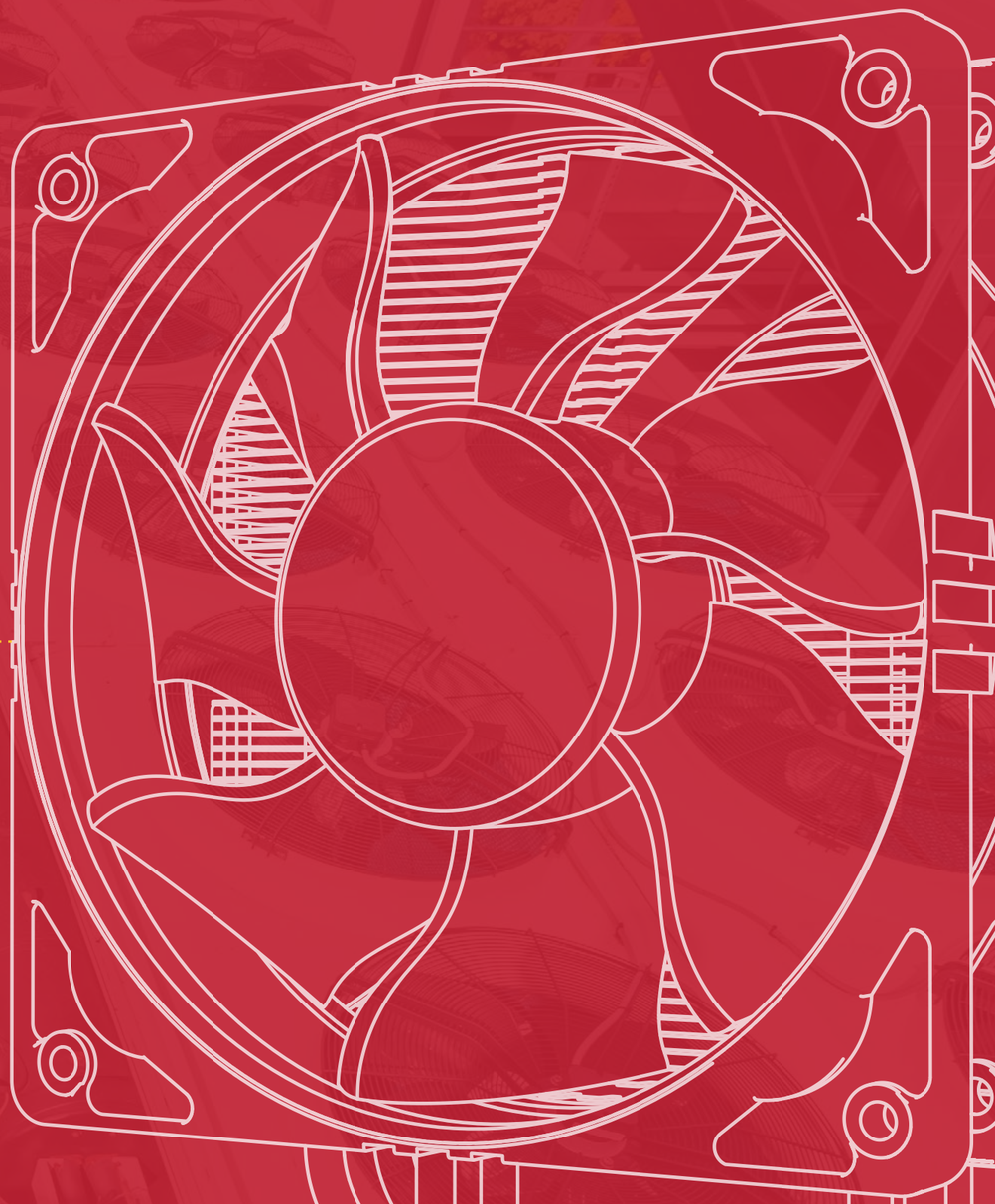
- Add and enforce multi-factor authentication.
- Strengthen credentials, especially passwords to secure remote connections.
- Use granular user and role-based access control policies.

Defining Responsibilities

- Adhere to a shared responsibility model and define a line between an organization's and the cloud provider's responsibilities.

ABOUT THE STATE OF XIoT SECURITY REPORT





ABOUT THE STATE OF XIoT SECURITY REPORT

Claroty Team82's biannual State of XIoT Security report is a deep examination and analysis of connected device vulnerabilities disclosed during the first half of 2022 affecting industrial, healthcare, and commercial products.

Throughout this report, you'll learn about vulnerabilities impacting industrial control systems, the internet of medical things (IoMT), building automation systems, and enterprise internet of things (IoT) devices that sustain our lives and enable innovation across business and critical infrastructure sectors.

Recognizing the critical need to understand the XIoT risk and vulnerability landscape, Team82 developed an automated collection and analysis tool that ingests 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.

ABOUT TEAM82

Team82, the research arm of XIoT cybersecurity company Claroty, is an award-winning group of OT researchers known for its development of proprietary threat signatures, OT protocol analysis, and discovery and disclosure of industrial, healthcare, and commercial vulnerabilities.

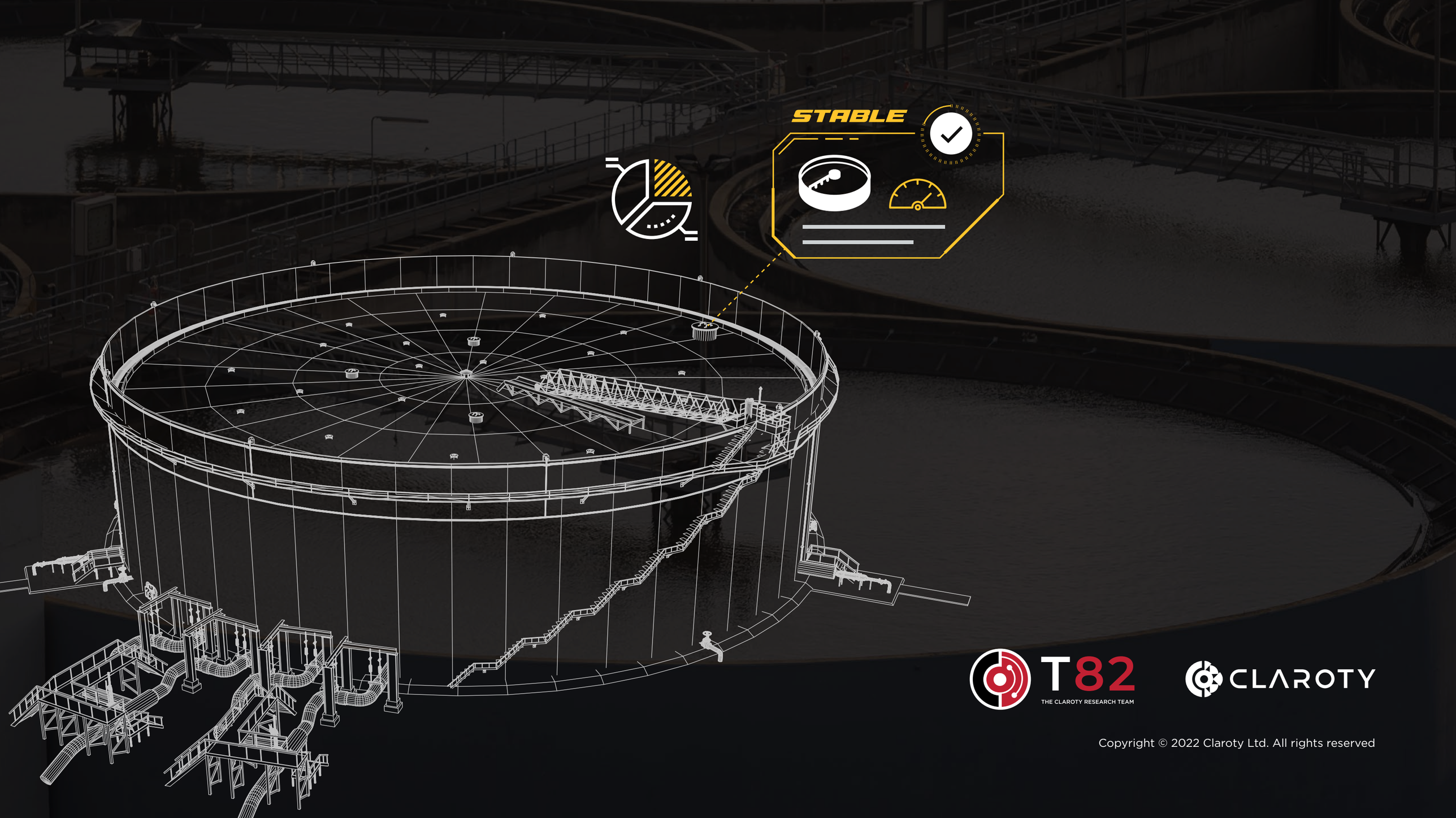
Fiercely committed to strengthening OT security and equipped with the industry's most extensive ICS testing lab, the team works closely with leading industrial automation vendors to evaluate the security of their products. As of August 2022, Team82 has discovered and disclosed 335 vulnerabilities.

For more information, visit: https://claroty.com/team82/

ACKNOWLEDGEMENTS

The primary authors of this report are Bar Ofner, security researcher at Claroty, and Chen Fradkin, data scientist.

Contributors include: Rotem Mesika, threat and risk group lead, Nadav Erez, director of innovation, Sharon Brizinov, director of research, and Amir Preminger, vice president of research. Special thanks to the entirety of Team82 for providing exceptional support to various aspects of this report and research efforts that fueled it.



T82
THE CLAROTY RESEARCH TEAM

CLAROTY