

A low-angle, upward-looking photograph of a large industrial facility, likely a refinery or chemical plant. The image is dominated by a tall, silver, cylindrical smokestack on the left side, which rises towards the top of the frame. To the right and in the foreground, there is a complex network of industrial structures, including multiple levels of steel walkways, ladders, and a dense array of horizontal and vertical pipes. The pipes are wrapped in silver insulation. The sky is a clear, bright blue with some light, wispy clouds. A warm, orange-yellow light flare is visible in the center of the image, creating a sense of depth and highlighting the metallic surfaces. The overall composition emphasizes the scale and complexity of the industrial infrastructure.

POSITIVE TECHNOLOGIES

ICS VULNERABILITIES: 2018 IN REVIEW

Contents

- Introduction..... 2
- Abbreviations..... 2
- Analysis of vulnerabilities in ICS components..... 3
 - Materials and methods 3
 - Trends..... 3
 - Vulnerabilities published in 2018: distribution by manufacturer 4
 - Vulnerabilities by component type 4
 - Vulnerabilities by types..... 5
 - Vulnerabilities by impact 5
 - Distribution of vulnerabilities by severity 6
- Availability of ICS components on the Internet..... 7
 - Materials and methods 7
 - Prevalence 7
 - Geographic distribution 8
 - Distribution by vendors and products..... 8
 - Types of ICS components..... 8
- Conclusion..... 9

Introduction

2018 was rich in ICS incidents. Details were published regarding use of the Triton cyberweapon, which, like Stuxnet and Industroyer, targets ICS equipment. In addition, several high-profile attacks struck industrial companies. Boeing announced it was hit by WannaCry and a few months later, the same virus shut down several plants of Taiwan Semiconductor Manufacturing Company. Although the attacks targeted IT infrastructure, their consequences also affected operational technology used for production. In effect, attackers do not always need specific knowledge about a target's operations in order to disrupt them.

After exploiting vulnerabilities in the IT infrastructure, hackers can gain access to the industrial network. According to our research, an internal attacker already on the corporate information system would have been able to penetrate the industrial network in 82 percent of cases. At that point, the attacker has a number of ways to perform malicious acts against ICS components, and the most common one is to exploit known vulnerabilities. That is why it is so important to know about the vulnerabilities existing in ICS equipment, as this allows businesses to assess the risks in time and take appropriate protection measures.

This research outlines known vulnerabilities in ICS components and the availability of such components on the Internet, with data to show how the situation has evolved over the last few years.

Abbreviations

DCS	distributed control system
HMI	human-machine interface
ICS	industrial control system
PLC	programmable logic controller
RTU	remote terminal unit
SCADA	supervisory control and data acquisition

Analysis of vulnerabilities in ICS components

Materials and methods

Information was drawn from publicly available sources, such as vulnerability knowledge bases, vendor advisories, scientific papers, and posts on security websites and blogs.

The following vulnerability knowledge bases were used:

- ICS-CERT (ics-cert.us-cert.gov);
- NVD (nvd.nist.gov), CVE (cve.mitre.org);
- Positive Research (securitylab.ru/lab).

The severity of vulnerabilities in ICS components was assessed based on the Common Vulnerability Scoring System (CVSS) version 3 (first.org/cvss).

Our research includes vulnerabilities published in 2018, as well as additional information about vulnerabilities found by our experts in 2018 and published in 2019.

We only considered vulnerabilities found in the equipment of leading manufacturers of ICS components.

Trends

The number of new vulnerabilities in ICS components rose by 30 percent compared to 2017. At the time of this research, complete information had been published about 243 vulnerabilities, with 14 vulnerabilities still pending analysis.

Detailed analysis of a device or system often reveals not just one but several vulnerabilities. For example, our experts uncovered 12 [vulnerabilities](#) in the APROL industrial control system from B&R Automation.¹

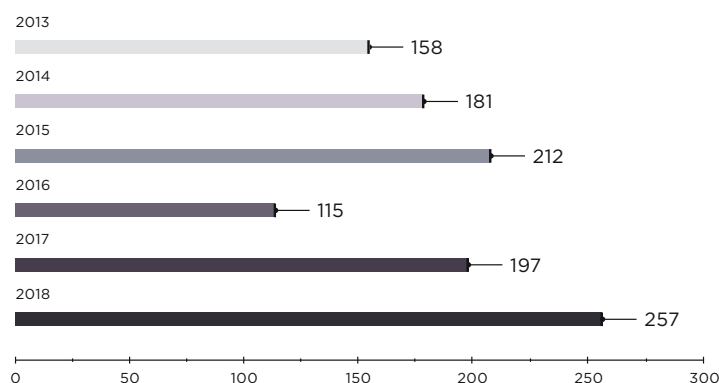


Figure 1. Total number of vulnerabilities found in ICS components

1. Part of ABB, a leading world manufacturer of industrial equipment, since July 2017.

Vulnerabilities published in 2018: distribution by manufacturer

Schneider Electric remained the leader in number of new vulnerabilities in 2018, even though the number of vulnerabilities found in Siemens equipment almost doubled compared to the previous year. The top spots of the two companies can be explained by their wide-ranging, popular product lines.

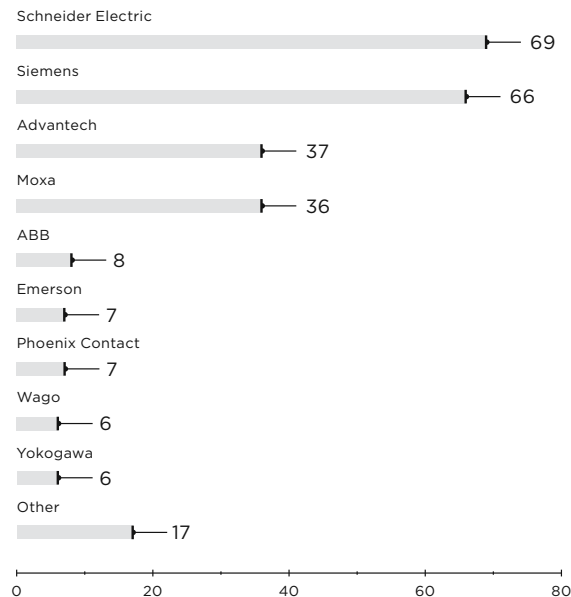


Figure 2. Vulnerabilities published in 2018: distribution by main ICS manufacturers

Vulnerabilities by component type

The distribution of vulnerabilities by ICS component type changed significantly in 2018. In 2017, the majority of vulnerabilities were found in HMI/SCADA components. But in 2018, vulnerabilities were almost evenly distributed among HMI/SCADA, PLC/RTU, and industrial network equipment.

The percentage of vulnerabilities in PLC/RTU components rose by 7 percent compared to 2017. Our experts found 10 vulnerabilities in PLC modules from Siemens and Schneider Electric.

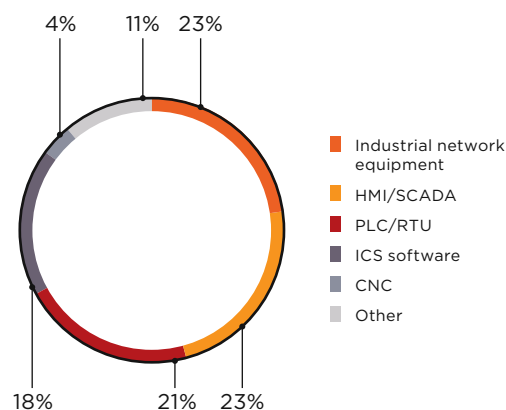


Figure 3. Vulnerabilities in ICS component types (percentage of vulnerabilities)

Vulnerabilities by types

A significant share of vulnerabilities involve improper authentication or excessive privileges. More than half of these vulnerabilities (64%) can be exploited remotely.

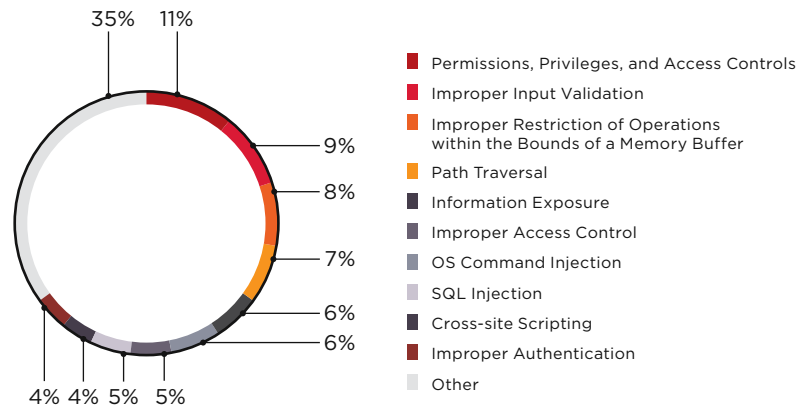


Figure 4. Types of vulnerabilities in ICS components

Vulnerabilities by impact

About 75 percent of vulnerabilities have the potential to affect ICS availability in full or part. Exploitation of these vulnerabilities, for example in network equipment, could disturb network communication and operations: network equipment is a key ICS element that shuttles commands between components.

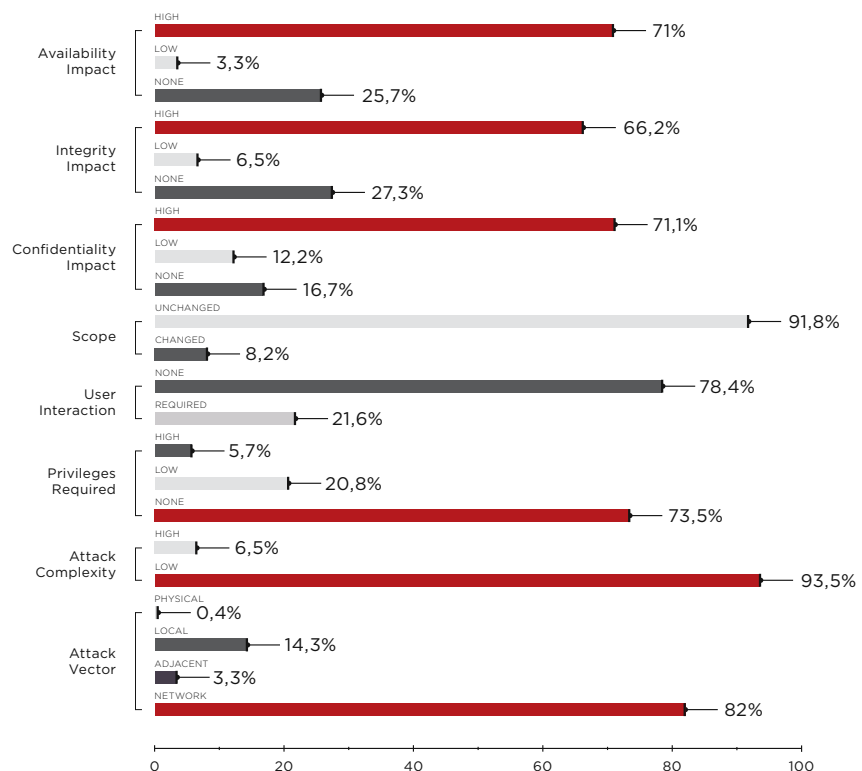


Figure 5. Vulnerabilities by CVSS metrics (percentage of vulnerabilities)

Distribution of vulnerabilities by severity

More than half of detected vulnerabilities were of critical or high severity, based on CVSSv3 scoring. Such vulnerabilities grew by 17 percent compared to the previous year. A high-severity vulnerability generally affects all three factors of information security: confidentiality, integrity, and availability. In 2018, 58 percent of vulnerabilities had this kind of three-part impact. And in only 4 percent of cases was the difficulty of exploiting them assessed as high. In other words, attackers do not usually require any special conditions to disrupt the security of ICS elements.

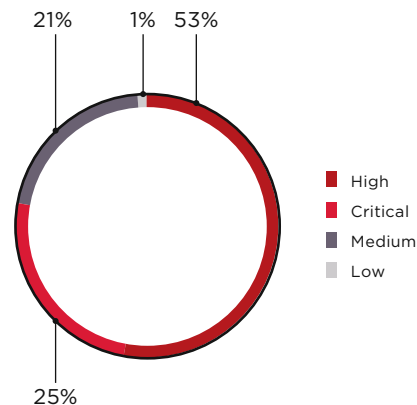


Figure 6. Severity of vulnerabilities

Summary of vulnerabilities in ICS components detected by Positive Technologies

In 2018 and early 2019, information about 54 vulnerabilities found by our experts was published. The vulnerabilities were detected in ICS components made by ABB, B&R Automation, Hirschmann, Moxa, Phoenix Contact, Schneider Electric, and Siemens. 14 of them were critical; 11 were of high risk.

For example, a vulnerability allowing to bruteforce credentials using the proprietary protocol on TCP port 4000 was detected in Moxa switches. The vulnerability allows obtaining control of the switch and, potentially, the entire industrial network. To obtain a patched version of the relevant firmware, end users must specially request it from the [vendor](#).

For more vulnerabilities found by our experts, see the Positive Technologies website: <https://www.ptsecurity.com/ww-en/analytics/threatscape/>.

Availability of ICS components on the Internet

Materials and methods

The researchers scanned Internet-accessible ports using publicly available search engines such as Shodan (shodan.io), Google, and Censys (censys.io). Shodan scans a certain number of ports from specified IP addresses, which have been blacklisted by some administrators and firewall manufacturers. Therefore, to extend the scope of analysis, we added data obtained using Google and Censys.

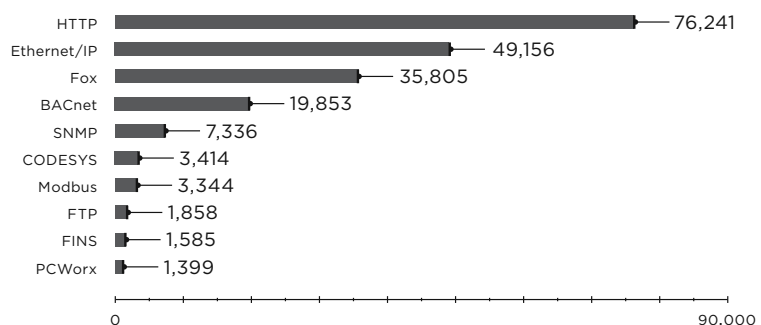


Figure 7. Number of Internet-accessible ICS components (top 10 protocols)

Prevalence

The research revealed 224,017 ICS components available online, which is 27 percent more than in 2017.

HTTP remains the most popular protocol. In 2018, experts detected 10,000 more ICS devices supporting HTTP than in 2017.

The number of devices supporting Ethernet/IP increased by 25 percent compared to 2017, making it the second-most common protocol (after HTTP). The number of devices on the Fox protocol declined by 9 percent.

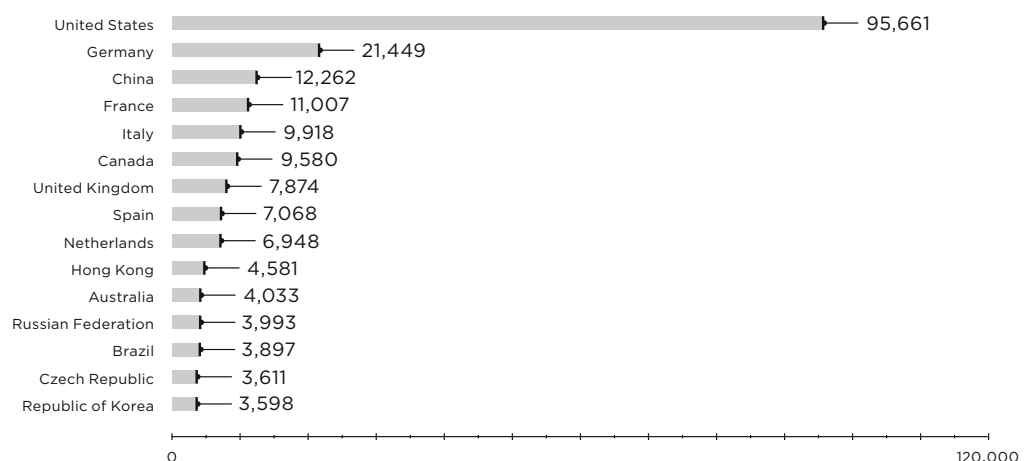


Figure 8. Number of Internet-accessible ICS components (top 15 countries)

Geographic distribution

Compared to 2017, distribution by country remained nearly identical. The U.S. still leads in the number of ICS components accessible online. The country's share grew by a third compared to the previous year, now accounting for 42 percent of the total. Russia rose from 28th place in 2017 to join the top 15 countries in 2018 at 12th place, with 3,993 devices.

Distribution by vendors and products

Distribution by vendors remained practically unchanged compared to 2017. At the time of this research, approximately 30,000 Honeywell devices were accessible. The number is only slightly higher than in 2017 (by around 7%), but the trend remains consistent from year to year. The share of Niagara Framework also slightly increased (by approximately 5%)

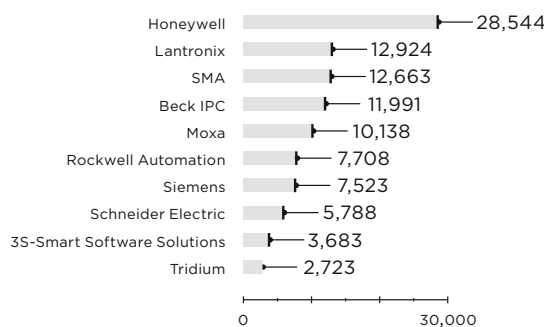


Figure 9. Number of Internet-accessible ICS components (top 10 vendors)

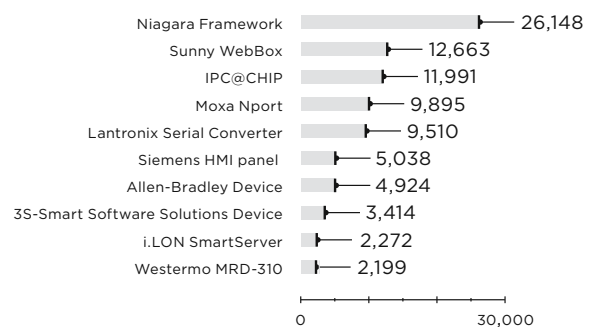


Figure 10. Number of Internet-accessible ICS components (top 10 products)

Types of ICS components

SCADA/HMI/DCS industrial control systems account for almost a third of Internet-accessible components (27%). The shares of network devices and PLCs increased by 6 percent (from 13% each in 2017)

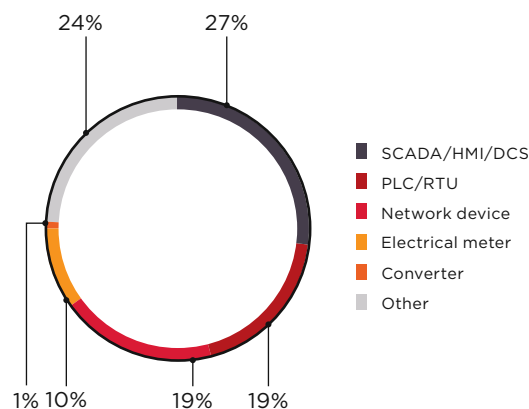


Figure 11. Number of Internet-accessible ICS components (distribution by type)

Conclusion

As our findings show, the number of vulnerabilities in the equipment of various manufacturers grows year after year, while the number of Internet-accessible ICS components does not diminish. The number of vulnerabilities in the products of leading manufacturers grew by 30 percent compared to 2017. The share of critical and high-severity vulnerabilities increased by 17 percent.

On average, vendors take a rather long time to fix vulnerabilities (more than six months). Elimination of some vulnerabilities—measured by time from vendor notification to release of a patch—can take more than two years. For end users, such protracted responses increase the risk of exploitation of device vulnerabilities.

More than 220,000 ICS components are available online, which is 27 percent higher than in 2017. Most of them are automation system components. Such systems are mainly located in the U.S., Germany, China, France, Italy, and Canada, even though lawmakers have long been concerned about the security of such devices and systems. For example, the International Organization for Standardization (ISO) has recently published new guidance to reduce the risks of cyberattacks on machinery.

Our research proves yet again that the security of ICS components has room to improve. Without constant attention and adequate protection, such components are at risk of being disrupted or disabled.

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

ptsecurity.com
info@ptsecurity.com

© 2019 Positive Technologies. Positive Technologies and the Positive Technologies logo are trademarks or registered trademarks of Positive Technologies. All other trademarks mentioned herein are the property of their respective owners.