ICS vulnerabilities increased in second half of 2020 as gaps in remote work expand attack surfaces

Throughout the second half (2H) of 2020, 71% of industrial control system (ICS) vulnerabilities disclosed were remotely exploitable through network attack vectors, according to the second Biannual ICS Risk & Vulnerability Report released today by Claroty, the industrial cybersecurity company. The report also revealed a 25% increase in ICS vulnerabilities disclosed compared to 2019, as well as a 33% increase from 1H 2020.

The report comprises the Claroty Research Team's discoveries alongside 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.

During 2H 2020, 449 vulnerabilities affecting ICS products from 59 vendors were disclosed. Of those, 70% were assigned high or critical Common Vulnerability Scoring System (CVSS) scores, and 76% do not require authentication for exploitation.

"The accelerated convergence of IT and OT networks due to digital transformation enhances the efficiency of ICS processes, but also increases the attack surface available to adversaries," said Amir Preminger, vice president of research at Claroty. "Nation-state actors are clearly looking at many aspects of the network perimeter to exploit, and cybercriminals are also focusing specifically on ICS processes, which emphasises the need for security technologies such as network-based detection and secure remote access in industrial environments. It is heartening to see a growing interest in ICS within the security research community, as we must shine a brighter light on these vulnerabilities in order to keep threats at arm's length."

Vulnerabilities on the rise in critical manufacturing, energy, and water and wastewater sectors

The critical manufacturing, energy, water and wastewater, and commercial facilities sectors—all designated as critical infrastructure sectors—were by far the most impacted by vulnerabilities disclosed during 2H 2020 and shows increases from the previous two years across the board:

Critical manufacturing increased 15% from 2H 2019 and 66% from 2H 2018Energy increased 8% from 2H 2019 and 74% from 2H 2018Water and wastewater increased 54% from 2H 2019 and 63% from 2H 2018Commercial facilities increased 14% from 2H 2019 and 140% from 2H 2018

Assessment of ICS vulnerabilities sees growth in third-party researchers

The number of ICS vulnerabilities disclosed in 2020 increased by more than 30% compared to 2018 and nearly 25% compared to 2019. Two factors contribute to this spike in recent years: a heightened awareness of the risks posed by ICS vulnerabilities, and researchers and vendors increasingly focused on identifying and remediating security flaws as effectively and efficiently as possible. This growth indicates security research focused on ICS products is maturing.

Third-party researchers were responsible for 61% of discoveries, many of which were cybersecurity companies. This signals a change in focus to include ICS alongside IT security research, which is further evidence of the accelerated convergence between IT and OT. Among all third-party discoveries, 22 reported their first disclosures, a positive sign of growth in the ICS vulnerability research market.

The Claroty Research Team discovered and disclosed 41 vulnerabilities during 2H 2020, affecting 14 vendors. These represent the direction and core objectives of the team's research focus. Overall, Claroty researchers have found and disclosed more than 70 ICS vulnerabilities to date.

To access the complete set of findings, in-depth analysis, and additional steps to defend against improper access and risks, download the Claroty Biannual ICS Risk & Vulnerability Report: 2H 2020.

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.

Contacts

Melissa Johnson
+61 2 9212 3888
mailto: mjohnson@primary-pr.com
Elaine Banoub
02 92123888
mailto: ebanoub@primary-pr.com