BLOG

ICS Cybersecurity in 2026: Vulnerabilities and the Path Forward

Rob Hulsebos, Daniel dos Santos, and Forescout Research - Vedere Labs | February 19, 2026

Share This:

Key Findings

Record Volume & Rising Severity

- 2025 set a record: 508 ICS Advisories covering 2,155 CVEs
- Average CVSS score has climbed to 8.07
- The average CVSS score is up 25% from 6.44 in 2010
- 82% of advisories reached high or critical severity

Most Vulnerable Assets

Sector Impact

- Manufacturing, energy, and transportation face the highest risk
- Healthcare surged from 8th to 4th most affected sector

Gaps

- 134 vendors published ICS vulnerabilities without associated CISA advisories
- CISA tracked only 22% of these vendor-published vulnerabilities
- 61% of non-CISA vulnerabilities carried high or critical severity
- Manufacturing and energy sectors remain primary targets

Mitigation Recommendations

- Expand vulnerability sources beyond CISA advisories
- Monitor vendor disclosures directly to capture the full threat landscape affecting your network

---

CISA/ICS-CERT has been the authoritative source about vulnerabilities in operational technology/industrial control systems (OT/ICS) since they started the ICS Advisory (ICSA) program in 2010.

Between March 2010 and January 31, 2026, CISA/ICS-CERT published 3,637 ICS advisories about 12,174 vulnerabilities affecting 2,783 products from 689 vendors. One hundred seventy eight (178) of these advisories were dedicated to medical devices — nearly 5 %.

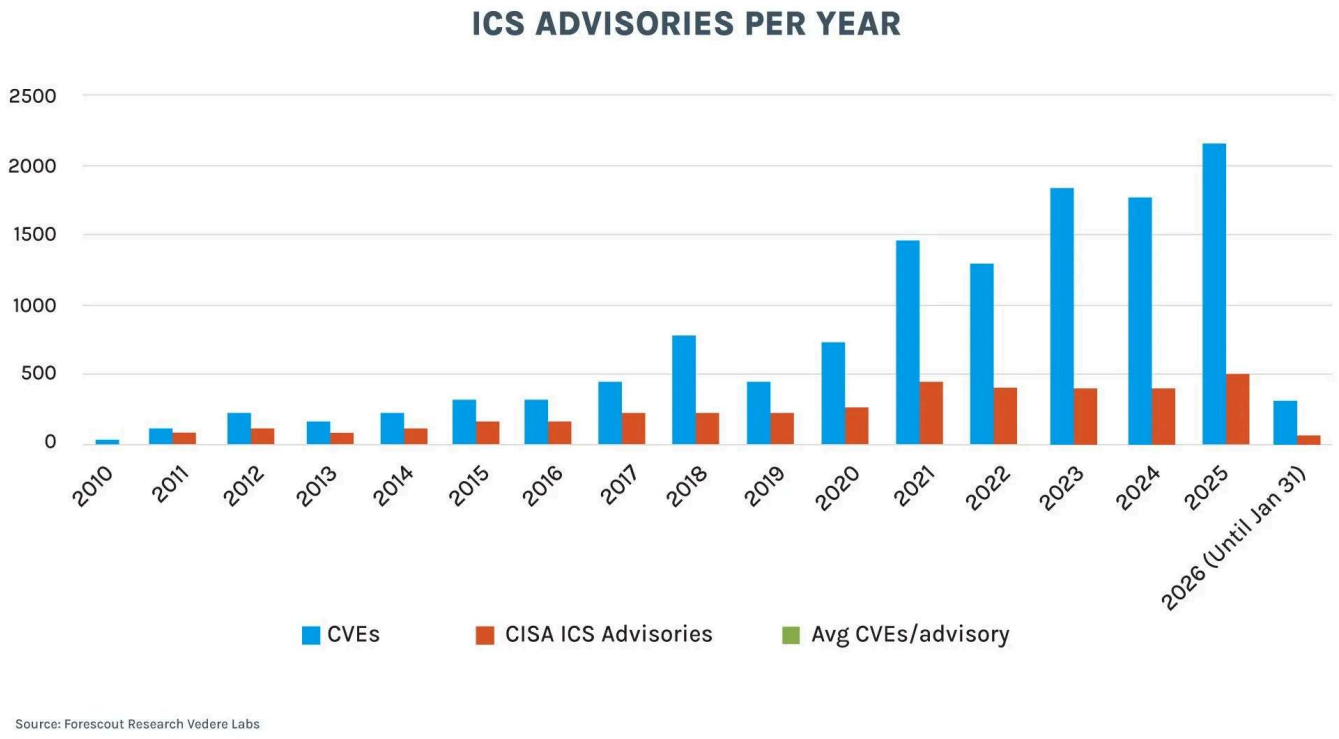
However, there is a growing number of vulnerabilities on critical devices that are not tracked with associated ICSAs which may leave asset owners and network administrators with blind spots on their networks.

As reported in our 2025 Threat Roundup, the number of attacks on OT and critical infrastructure continues to grow, so it's crucial that asset owners improve visibility into their vulnerabilities to mitigate risks.

Where We Stand: ICS Cybersecurity Advisories Over the Years

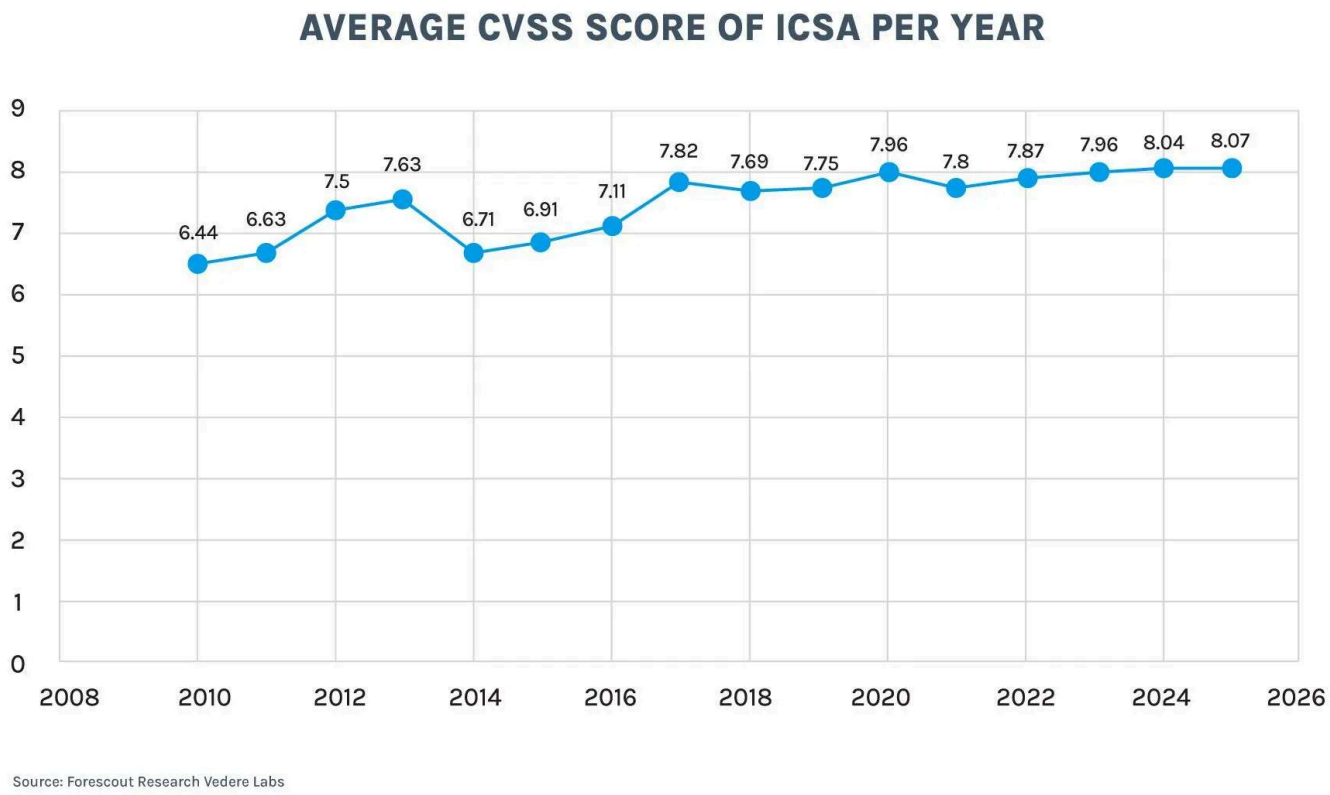
The chart below shows how the number of published OT/ICS advisories per year has been growing at an alarming rate:

- The first full year of ICS advisories, 2011, had 103 CVEs within 67 advisories for an average of 1.5 CVE per advisory.
- In 2025, there were 2,155 CVEs in 508 advisories for an average of 4.2.
- Last year was also the first time that CISA published more than 500 ICS advisories in a single year.

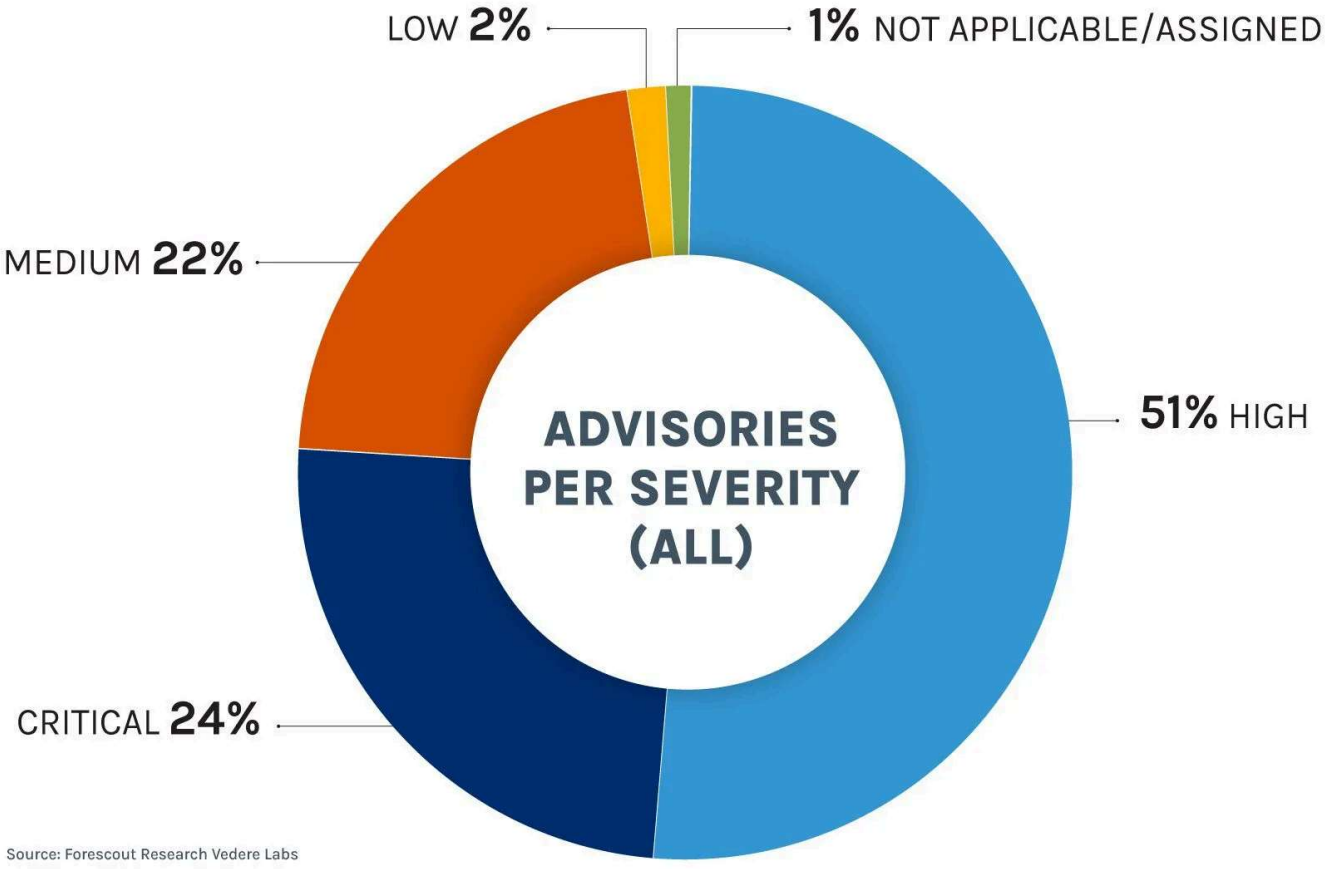


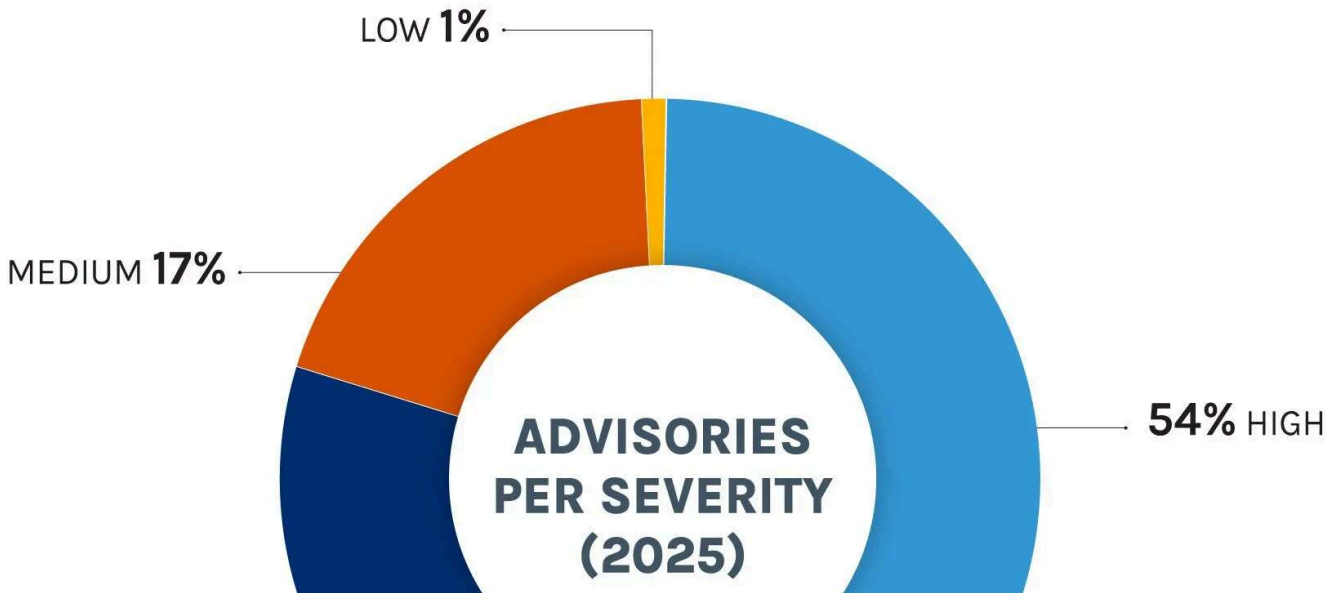
Source: Forescout Research Vedere Labs

The number of OT/ICS vulnerabilities isn't the only thing growing. They are also becoming more severe. The average CVSS score of advisories has been trending upwards (see



The CVSS distribution per severity category is shown below. If we look at all the published advisories, 75% of them were either high or critical. But if we isolate 2025, that number jumps to 82%.

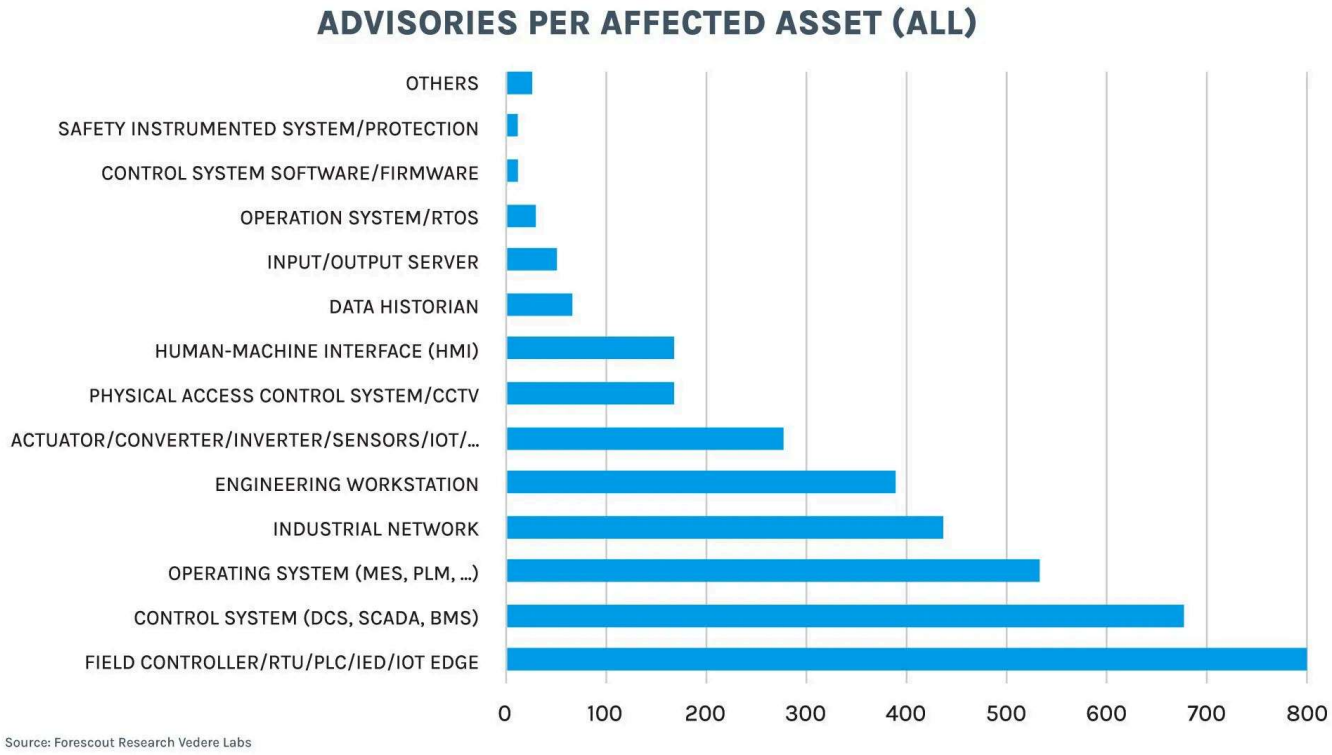


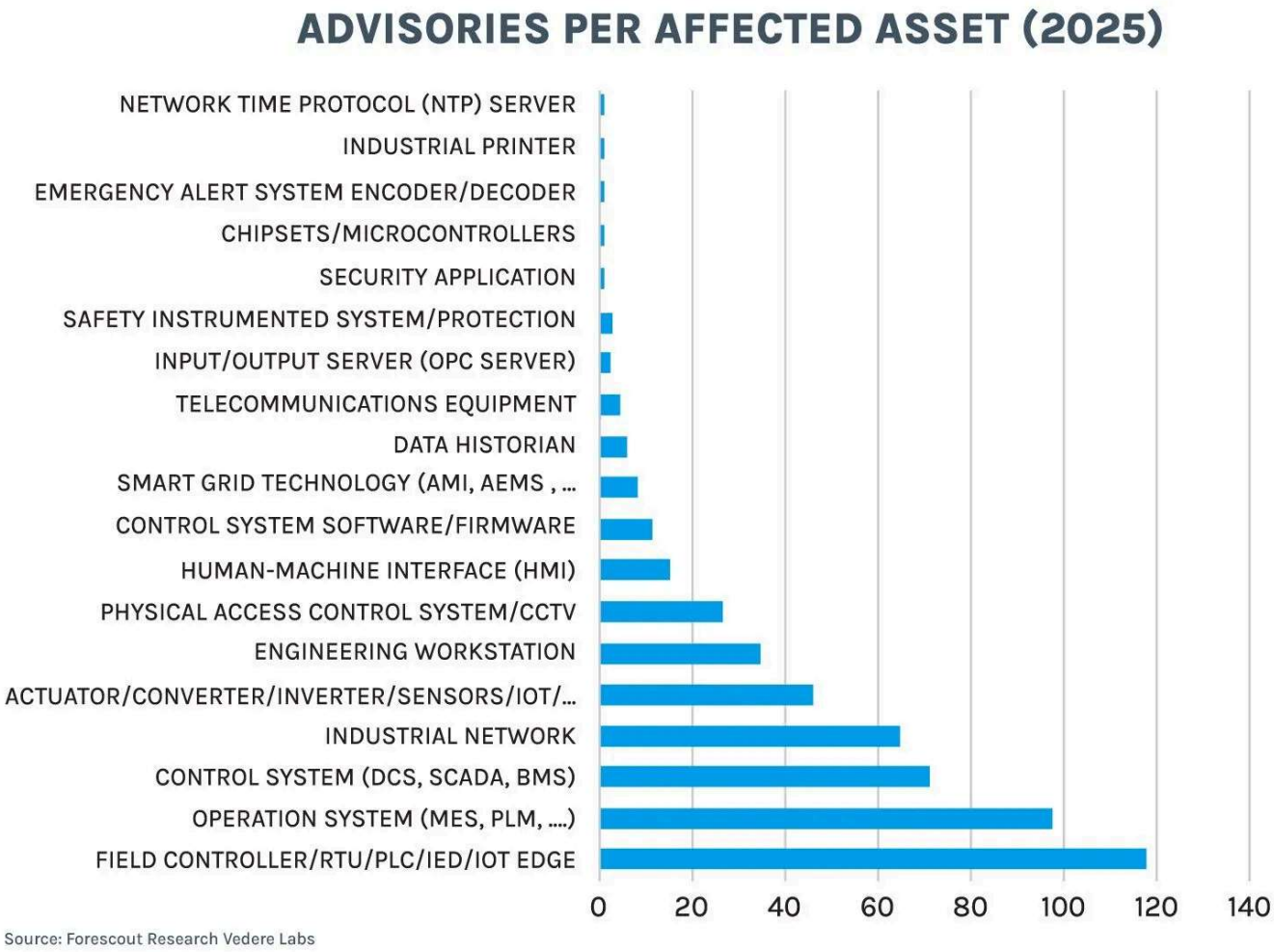


The following charts show the distribution of ICSA per affected asset type with the full dataset *and* with 2025 data only. The situation did not deviate significantly last year from the historical average. Most affected assets in 2025 were (in order):

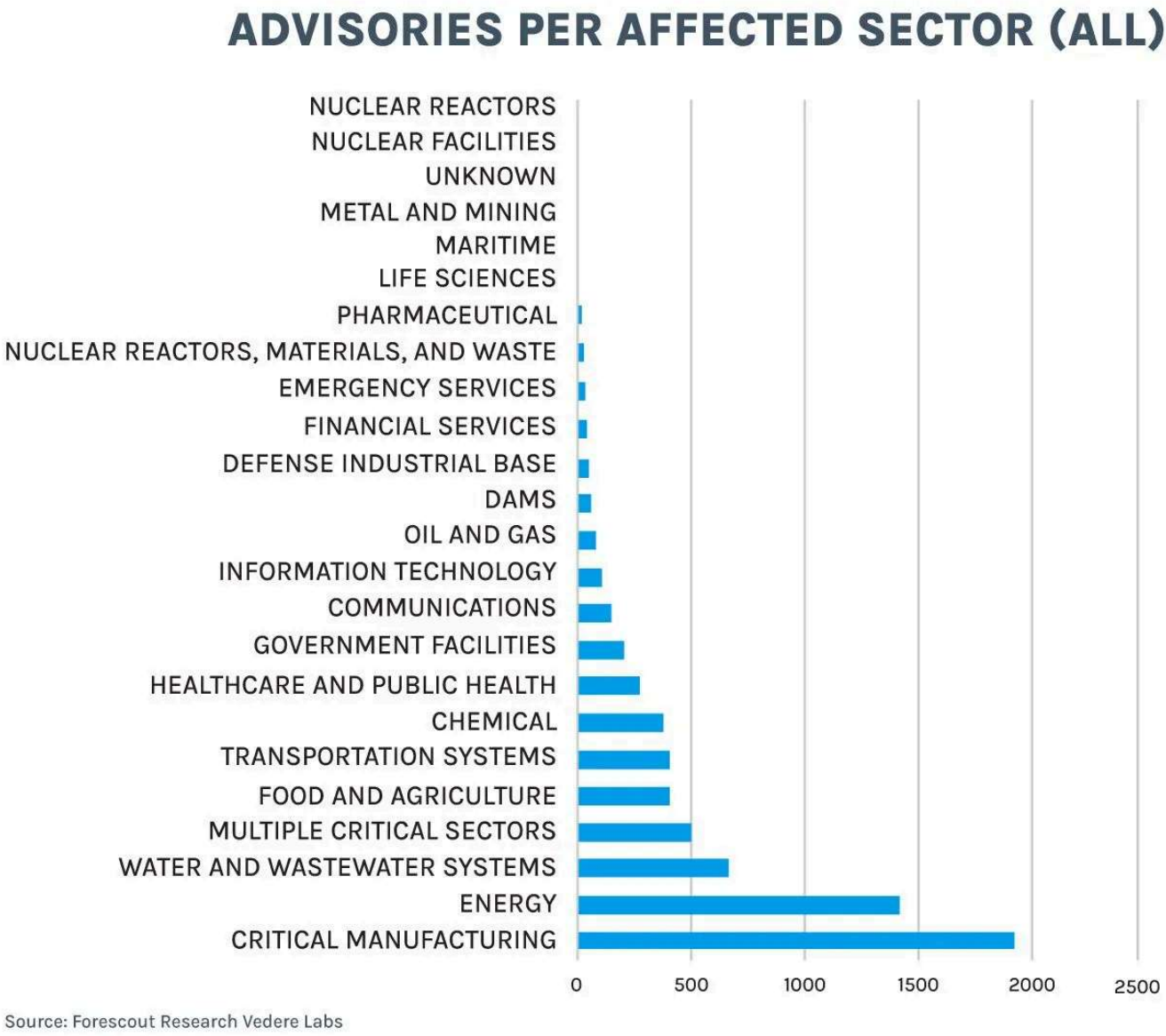
- Purdue Level 1 devices such as field controllers, RTUs, PLCs and IEDs
- Purdue Level 3 operation systems, such as MES, PLM, EMS and others
- Purdue Level 2 control systems such as DCS, SCADA and BMS

The fourth type of affected asset (summarized as 'industrial network') encompassing routers, firewalls, and other network infrastructure is also highly relevant. As we recently discussed, exposed industrial network infrastructure attracts even more attacks than exposed lower-level OT devices.

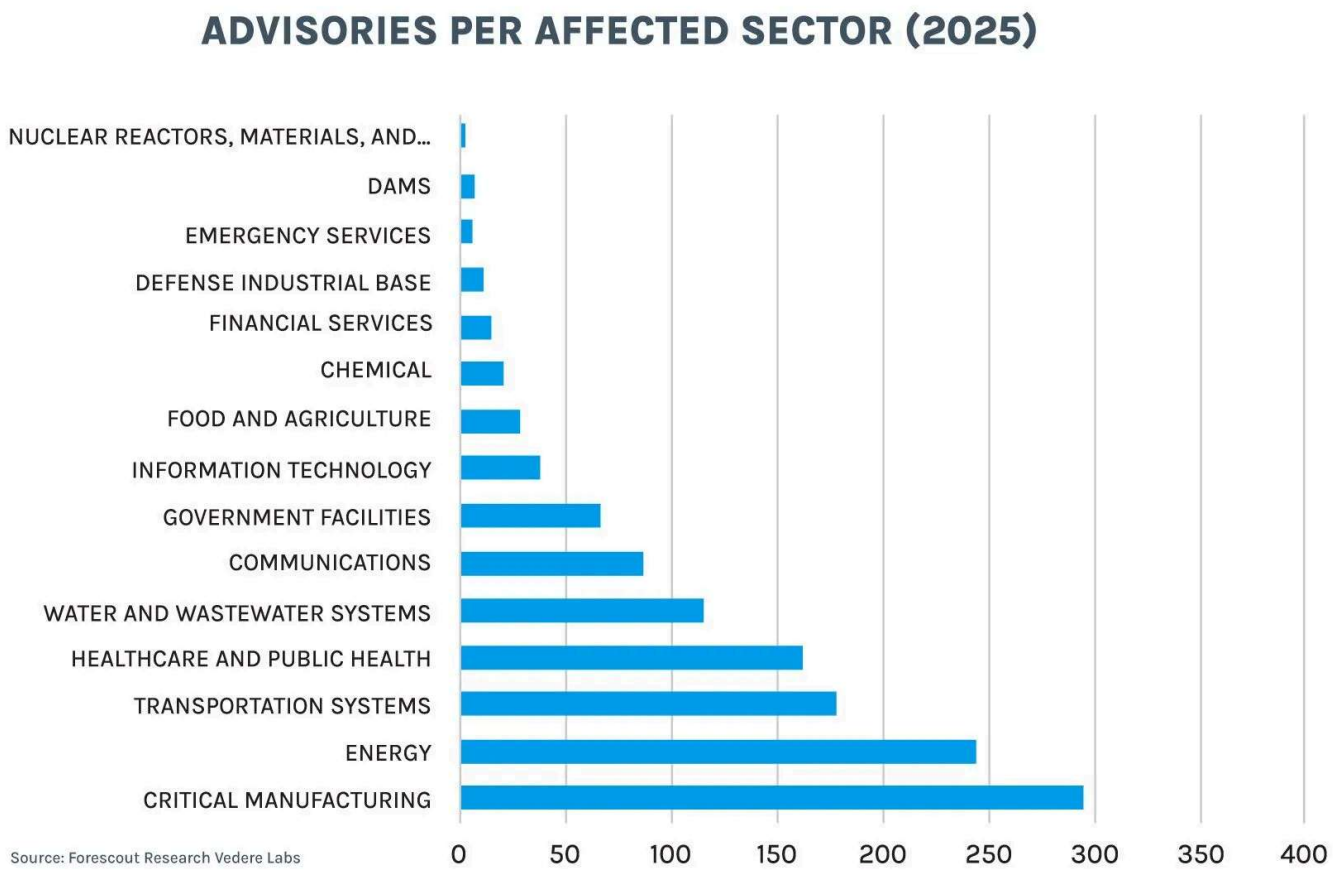




When we look at where these assets are used (as documented in ICSA publications), we see that manufacturing and energy have been the top two most affected sectors last year and over time. Historically, water and wastewater were the third most affected sector, but in 2025 that spot was taken by transportation. Another notable change is that healthcare jumped from the eighth most affected sector over time to fourth last year.



Source: Forescout Research Vedere Labs



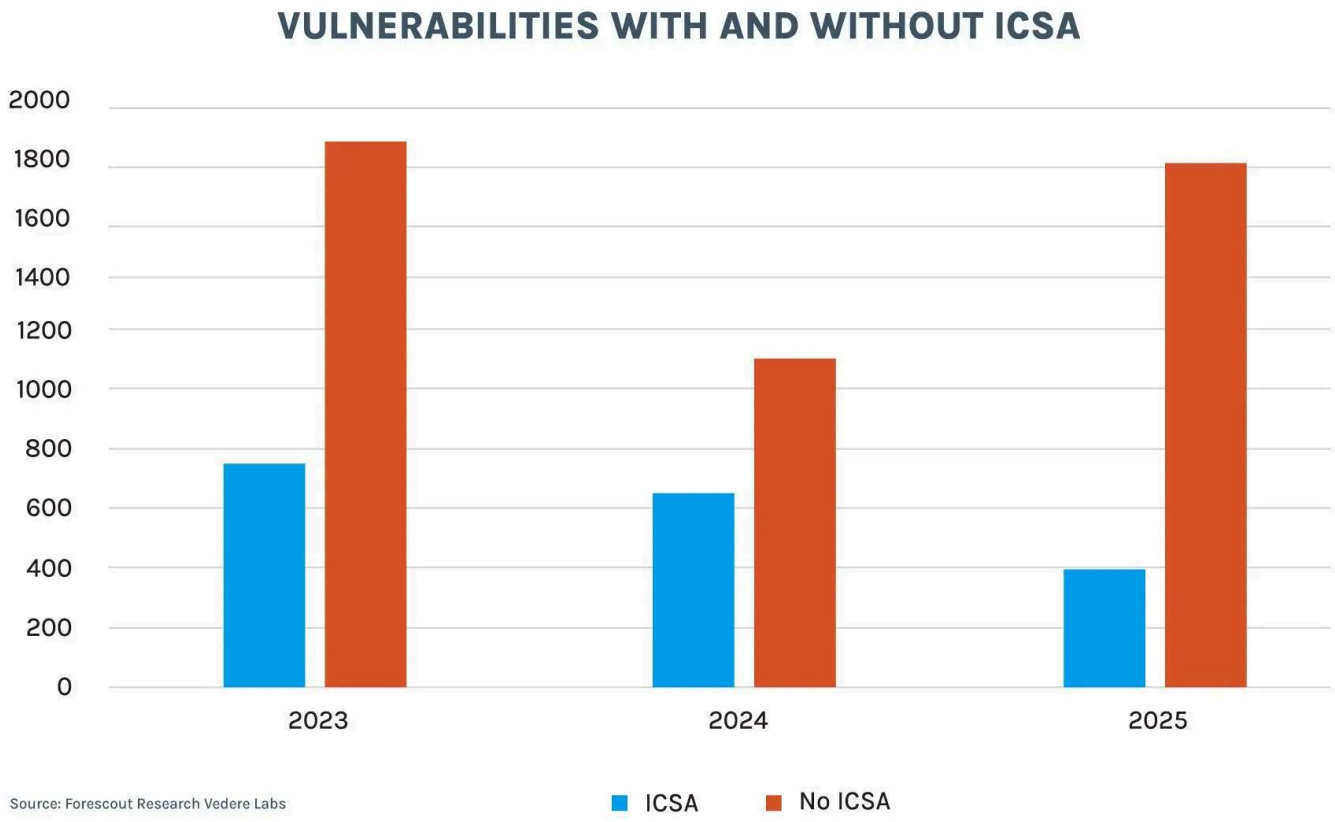
The figures above paint a picture of a growing number of vulnerabilities in OT/ICS, with increasing severity, affecting mostly critical assets in Purdue levels 1, 2, and 3 that are used in very critical sectors such as manufacturing, energy, transportation, healthcare, and water.

Unfortunately, that is only the tip of the iceberg.

Going Beyond CISA: Vulnerabilities Published by Vendors and Other CERTs

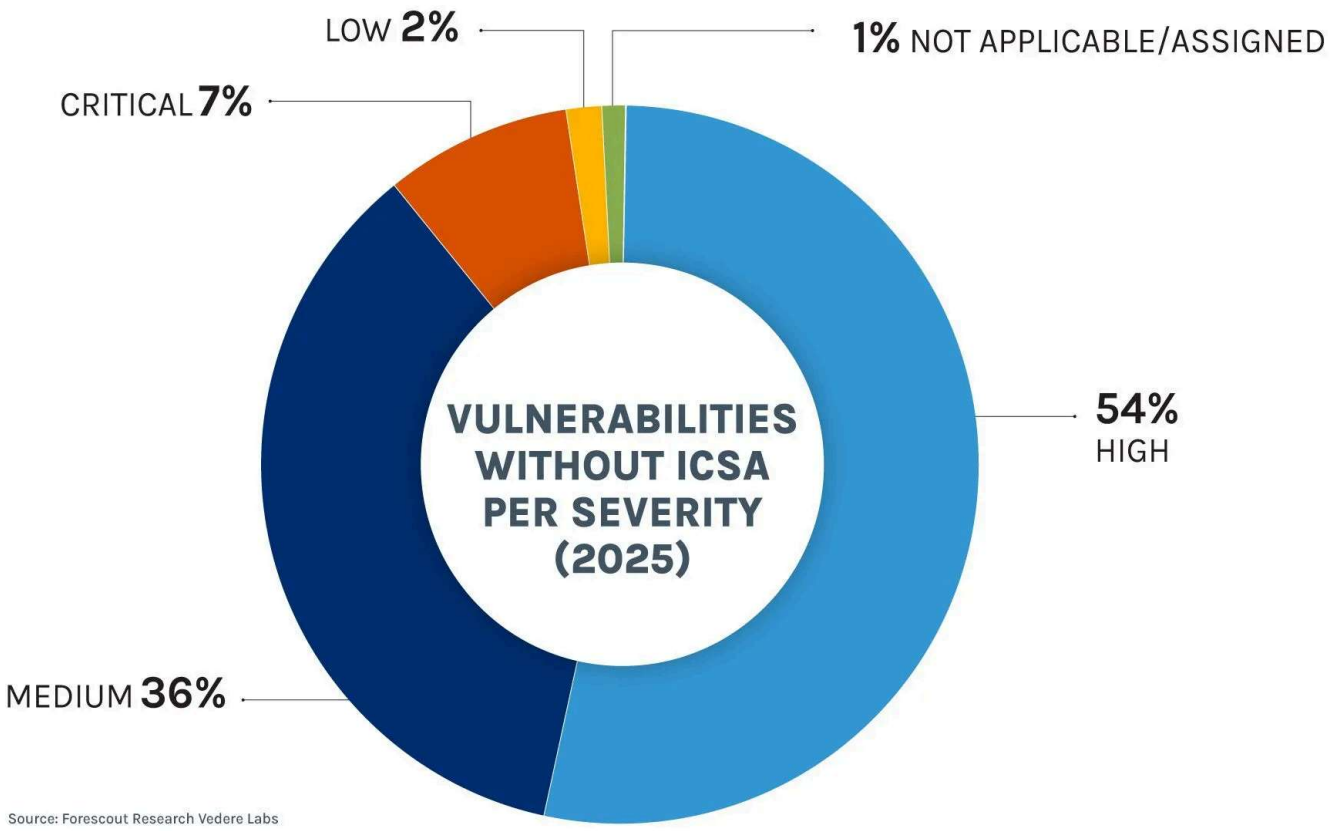
On January 10, 2023 CISA announced they would stop publishing updates on advisories affecting Siemens products, and instead, will be redirecting users to Siemens'

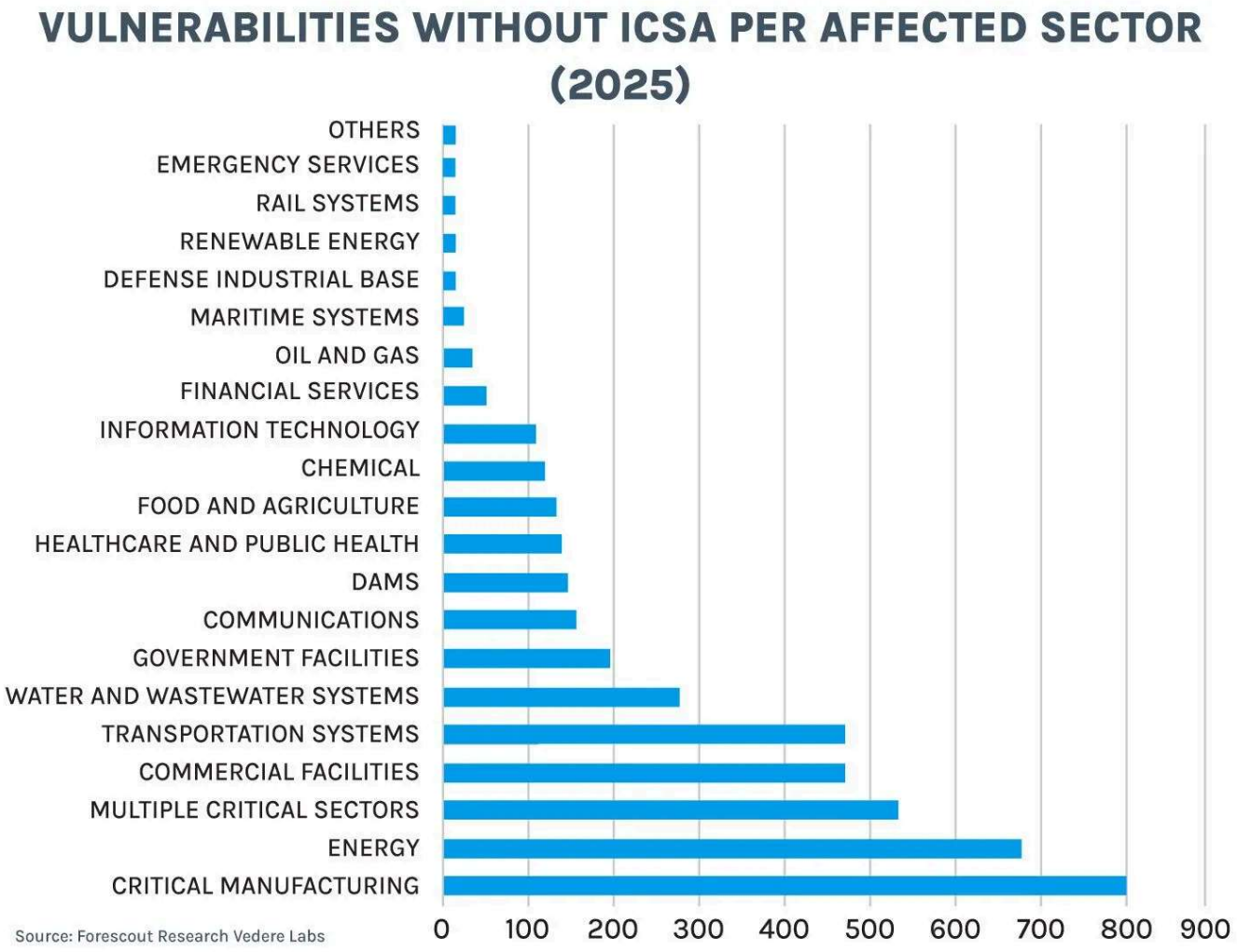
The ICS advisory project also tracks OT/ICS vulnerabilities published directly by 268 vendors and CERTs between January 1, 2023 and January 31, 2026. In this period, there were 6,737 published vulnerabilities, as broken down per year (see below).



Notice that in 2025, only 22% of these vulnerabilities had an associated ICSA published by CISA. That number was 58% in 2024 and 40% in 2023. There were vulnerabilities without an associated ICSA published by 134 vendors in 2025. Clearly, there a fair amount of OT/ICS risk that is not tracked by ICSAs.

Vulnerabilities without an ICSA are no less important than those with a dedicated advisory from CISA. In fact, 61% of vulnerabilities in 2025 without an ICSA had a high or critical severity. And like those vulnerabilities tracked by CISA, these mostly affected the manufacturing and energy sectors.





Turning the Tide: How Regulation and Industry Collaboration Are Transforming OT/ICS Vulnerability Management

'Patch Tuesday' is the day each month when Microsoft and other big tech companies release their software security updates. It is usually the second Tuesday of every month. More important than the day of the week is the security maturity of these vendors shown by the regularity of updates. This regularity allows system administrators and security

vendors and a regular cadence of available patches can help asset owners plan their risk assessment and mitigation activities.

In recent years, asset owners, end users, cybersecurity researchers, and government agencies have increasingly called for a greater focus on these specific OT/ICS vulnerabilities. The forthcoming EU Cyber Resilience Act (CRA) is already making an impact, encouraging vendors to take a more proactive approach to establish coordinated disclosure processes and release patches. The EU is not the only authority driving change through regulation. For example, Mitsubishi addressed a vulnerability due to requirements under Chinese cybersecurity laws last September.

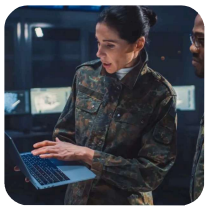
Even if some vendors are still unprepared for these changes, as evidenced by bad practices, such as silent patches (i.e., fixes with no CVE identifiers), many are embracing progress.

Several vendors now directly publish cybersecurity advisories for their own products — decreasing the exclusive reliance on the CISA/NVD ecosystem. This ecosystem offers the advantage of centralization but it's a single point of failure, as evidenced by the NVD backlog and funding crises of 2025. Another sign of progress is the publication of advisories in the machine-readable format CSAF which allows for automated parsing.

These gaps and the progress discussed here are the main reasons why Forescout's vulnerability database uses vendor advisories as a primary source of information in our OT-focused eyeInspect *and* across the entire Forescout 4D Platform™. That means the information is more complete, made available quicker, and does not carry the risk of typos or interpretation errors created when other parties copy vulnerability information in their own format.

Addressing the challenge of vulnerability management in OT/ICS requires a combination of regulatory pressure, industry collaboration, and vendor accountability. Increased transparency about patch timelines, dedicated resources for vulnerability management, and stronger incentives for rapid response could help accelerate the process across the sector. Additionally, fostering a culture of proactive security, rather than reactive fixes, would benefit vendors *and* asset owners.

Latest Blogs



How Continuous Assurance and UZTNA Help You Pass Government Audits

AI in Cybersecurity: The Future CISO Is an Augmented Leader

Securing Modern OT: Why Visibility, Cloud, and Hybrid Architectures Now Define Industrial Cybersecurity

Trending Topics

Healthcare Malware Hunt, Part 1: Silver Fox APT Targets Philips DICOM Viewers

Analysis: A New Ransomware Group Emerges from the Change Healthcare Cyber Attack

ICS Threat Analysis: New,