ICS/OT Vulnerability Intelligence Report Highlights Gap Between Severity Scores and Real-World Exploitation

EmberOT & partners release a vuln intel report, giving OT defenders a context-driven framework to cut through the noise of a record-breaking year of disclosures

EmberOT and partners release the OT Vulnerabilities Intelligence Report

CHANDLER, AZ, UNITED STATES, March 2, 2026 /EINPresswire.com/ -- EmberOT and partners have released the ICS/OT Vulnerability Intelligence Report 2024-2025, a comprehensive analysis of industrial control system vulnerabilities that challenges the conventional wisdom of score-based patch prioritization. The report's most striking finding: of 2,203 vulnerabilities scored High or Critical in 2024 and 2025, only 29, 1.32%, have ever been confirmed as weaponized in the real world.

> A scoring system designed for IT environments was never built to answer the question that matters most in OT: which vulnerabilities, in my specific architecture, matter right now?"
>
> *Jori VanAntwerp, EmberOT Founder & CEO*

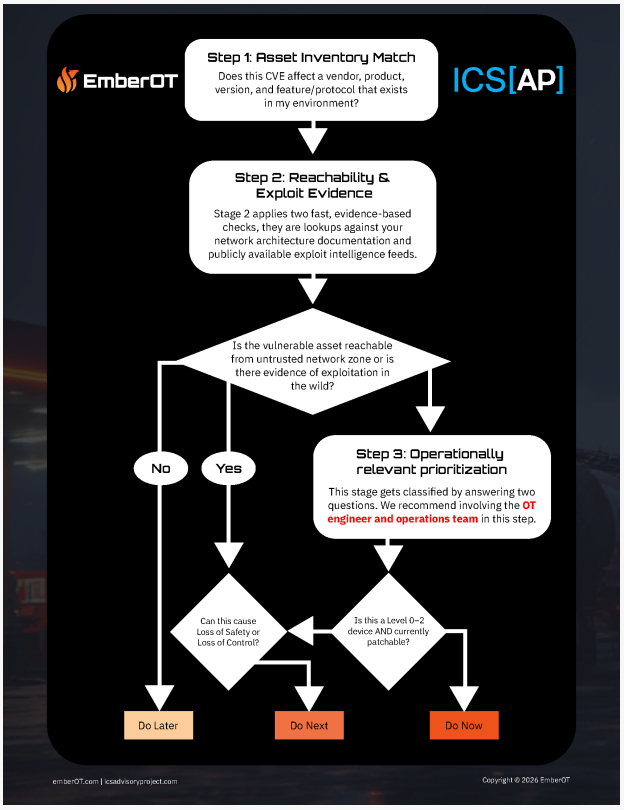
The report arrives at a pivotal moment. CISA (the Cybersecurity & Infrastructure Security Agency) published 508 ICS advisories in 2025 alone - a 20% increase over the previous year, while total tracked disclosures across all sources rose to 2,207. At the same time, the share of vulnerabilities receiving an official CISA advisory dropped from 28.3% in 2024 to just 17.5% in 2025, leaving the vast majority of disclosures invisible to organizations relying solely on federal feeds.

Key Finding: 98.4% of vulnerabilities scored High or Critical in 2024-2025 have never been confirmed as exploited in the wild, yet they continue to consume the majority of OT security teams' bandwidth.

"OT defenders are protecting more than just data... They're protecting process, safety, and

business continuity," states Jori VanAntwerp, Founder at EmberOT. "A scoring system designed for IT environments was never built to answer the question that matters most in OT: which vulnerabilities, in my specific architecture, matter right now? This report gives teams the framework to answer that question with confidence."

EmberOT - Visibility and Security for Critical Infrastructure



The report includes a printable vuln prioritization flowchart

A Prioritization Crisis, not a Data Crisis

The report, authored by Dan Ricci (Founder, ICS Advisory Project), Jori VanAntwerp (Founder, EmberOT), and Dr. Rishabh "George" Das (Independent OT Security Researcher), argues that the industrial security community's challenge is not a lack of vulnerability data, but rather the absence of a structured, operationally grounded framework for determining which vulnerabilities actually warrant action.

Drawing on the ICS Advisory Project's tracking of more than 82% of advisories that never appear in official CISA ICS channels, the report introduces a five-lens prioritization framework built around exploitability, network reachability, asset criticality, operational impact, and patch feasibility. The framework is designed to replace CVSS-score-driven triage with environment-specific risk assessment that OT teams can document and defend.

"The gap between what gets reported and what gets fixed has never been wider," notes VanAntwerp. "That's more a prioritization problem than a resourcing problem. This report exists to give every operator, from the smallest municipal utility to the largest enterprise, the intelligence they need to make better decisions."

Key Findings at a Glance

The report covers 2024 and 2025 disclosure data and surfaces findings with direct operational implications:

• The 1.3% Rule: Of 2,203 High/Critical CVEs tracked, only 29 (1.32%) appear in CISA's Known Exploited Vulnerabilities catalog. The other 98.4% have never been confirmed as weaponized.

• CISA Coverage in Decline: The proportion of vulnerabilities tracked by official CISA ICS Advisories fell from 28.3% in 2024 to 17.5% in 2025 - a 10.8-point drop in a single year.

• The Medium Surge: Medium-severity CVEs nearly doubled year over year (558 to 1,044+), reflecting the multi-year nature of the disclosure lifecycle and warning against treating annual counts as static snapshots.

• EOL and Patch Reality: 45% of advisories recommended hardware upgrades as the remediation path; 7.5% identified assets as End-of-Life with no fix forthcoming, making compensating controls a permanent architectural necessity for many operators.

• Level 1 in the Crosshairs: The highest concentration of network-reachable, low-complexity vulnerabilities resides at Purdue Level 1 - the PLCs and RTUs that directly control physical processes. 1,145 vulnerabilities in this category were identified at this level alone.

• High Disclosures ≠ Insecure Products: Vendors with the highest CVE counts, including Siemens (282 advisories) and Rockwell Automation (104), reflect mature PSIRT infrastructure, not weaker products. A vendor with zero CVEs may simply lack the processes to find what they have.

The Structural Gap: The Immune System That Was Never Built

Beyond the prioritization framework, the report identifies a critical gap in the current OT defense-in-depth strategy: over 80% of official guidance in the 2024-2025 period focused on network segmentation, while less than 1% addressed validation of the actual content of industrial traffic in real time.

The report introduces the concept of the "immune system" protocol-level content validation capable of detecting malformed or malicious traffic before it reaches a vulnerable device, without requiring a patch or hardware replacement. For the significant portion of the asset owner community running End-of-Life equipment or operating under constrained maintenance windows, this layer represents the only remaining path to meaningful risk reduction.

ICS/OT Vulnerability Intelligence Report Availability

The ICS/OT Vulnerability Intelligence Report 2024-2025 is available now at https://emberot.com/ics-ot-vulnerability-intelligence-report-2024-2025. A companion practitioner guide, No Noise. Just Signal: A Practitioner's Guide to OT Vulnerability Prioritization, containing worked examples, documentation templates, and a repeatable triage process, is forthcoming.

—

 About EmberOT

EmberOT solves critical infrastructure security challenges by meeting organizations where they are today. Where predecessor solutions are hardware-dependent and cost-prohibitive, EmberOT's software-based sensors remove those barriers and help organizations monitor and defend their environments NOW while showing them a path to the FUTURE. Combining secure by design with defense in depth, the EmberOT software provides immediate observability and detection, actionable insights, and guidance on "What should I do next?" to ensure critical infrastructure resilience and security. Learn more at https://www.emberot.com/.

Sonia Awan for EmberOT
Outbloom Public Relations
email us here
Visit us on social media:
LinkedIn
YouTube
X