Hey! What's New? 2026-51

The Most Vulnerable AI Products Are Also Some of the Most Commonly Exposed Online

The most vulnerable AI products are also some of the most commonly exposed online, says Eric Geller in *Cybersecurity Dive*. "Not only are AI services increasingly appearing on the public internet, but the products with the most significant vulnerabilities are the ones popping up most frequently."

"North America accounts for the most internet-exposed industrial control systems (ICS) as of early 2026, with roughly 38% of all such devices located on the continent," Geller says, "according to the internet monitoring firm Censys."

Meanwhile, the number of publicly accessible AI tools is growing fast, he adds, noting that "Censys detected more than 294,000 IP addresses associated with AI services in early 2026, up from 183,000 in October 2025." The data, from a preview of Censys's annual internet exposure report, "highlights the vast array of targets available to hackers who are intent on sabotaging critical infrastructure or subverting the AI tools on which companies increasingly rely."

Geller notes that Censys detected 169% more instances of the AI agent-building tool Langflow over the past nine months, "even as the software accumulated 18 vulnerabilities (14 of them scored as high-severity, four of them seeing exploitation) since 2024."

"Multiple unauthenticated remote code execution (RCE) vulnerabilities make any Internet-exposed instance a critical finding," Censys said.

Censys found that the number of internet-exposed instances of another common AI tool, LiteLLM, nearly doubled during its observation window, "even as hackers continue exploiting a pre-authentication SQL injection vulnerability. LiteLLM serves as a unified hub for connecting to commercial LLMs, meaning that a compromise of its data would expose a customer's API keys for all of those services."

For Geller, the ICS landscape, as it appears in Censys's data, is no less alarming. "The number of internet-exposed ICS devices has grown from 129,000 in 2024 to 138,000 in early 2026, magnifying the danger facing communities around the world as the equipment powering their energy grids, hospitals and water supplies remain within easy reach of hackers."

He then notes that, "while the lion's share of those devices are in North America, the number of systems in Asia has grown over the past two years, from 23% in 2024 to 27% in early 2026. The share in Europe dropped slightly, from 36% to 31%."

Other aspects of the ICS environment remain consistent. "Roughly 70% of hosts running ICS devices and services globally are consistently found on consumer and mobile networks for the last 2.5 years," Censys said. Business networks and cloud platforms account for significantly smaller shares; Censys did not specify their percentages, but a chart suggests that they are around 25% and 5%, respectively.

Learn more at [The State of the Internet Is Changing: AI Exposures Surge While Global ICS Trends Shift - Censys]().