Power Grids, Hospitals, and 911 Systems at Risk as CVE Funding Expires

Loss of CVE program would cripple vulnerability coordination across critical infrastructure, raising the risk of cyberattacks with life-threatening consequences

COLUMBUS, OH, UNITED STATES, April 16, 2025 /EINPresswire.com/ -- Matt Santill, cybersecurity executive, former CISO, and original contributor to the NIST Cybersecurity Framework, is sounding the alarm as the industry stands on the edge of a serious disruption: the imminent shutdown of the Common Vulnerabilities and Exposures (CVE) program due to federal funding lapses.

“A month ago, I warned the industry was heading for a major shakeup. Now, we’re here,” said Santill. “MITRE’s contract to operate the CVE program ends within a day, and unless Congress steps in immediately, the backbone of global vulnerability coordination will be lost.”

What Is CVE and Why Does It Matter?

The CVE program, operated by MITRE and funded by the U.S. government, provides a standardized system for identifying, naming, and cataloging known cybersecurity vulnerabilities in software and hardware.

“Think of CVEs like the license plate numbers of vulnerabilities,” Santill explains. “They allow companies, governments, researchers, and defenders around the world to coordinate when a new threat is found.”

Each time a vulnerability is discovered—whether in Windows, hospital equipment, routers, or water treatment systems—it receives a CVE ID. This allows:

•Security vendors to issue patches
•Cybersecurity teams to prioritize which flaws to fix
•Governments and regulators to track risk across industries
•Emergency response systems to know what software may be at risk

Without CVEs, there is no universal language for coordinating vulnerability response. The result?

Confusion, duplication, and delay—all of which favor attackers.

Impacts on Critical Infrastructure and Public Safety

The CVE program is especially crucial for protecting the systems Americans rely on every day. Sectors at risk if the program goes dark include:

•Power grids and energy systems – Vulnerabilities in substation control software or remote access tools used by grid operators could go untracked, leading to wide-scale blackouts. A similar risk was seen during the Colonial Pipeline attack, which used a known vulnerability to disrupt fuel supply across the East Coast.

•Water treatment and sanitation – A delayed or missed disclosure in a PLC (programmable logic controller) used for chemical treatment could allow threat actors to alter chlorine or fluoride levels in drinking water. A real-world incident occurred in Oldsmar, Florida, where an attacker attempted to poison a water supply remotely.

•Hospitals and medical equipment – Many hospital systems rely on CVEs to prioritize patching for life-saving equipment and healthcare software. In 2017, the WannaCry ransomware attack, which exploited CVE-2017-0144, caused chaos in the UK's NHS, forcing hospitals to cancel surgeries and divert ambulances.

•Airports and transportation – Baggage handling systems, flight control software, and even airport security systems depend on regular vulnerability intelligence. A failure to patch a disclosed CVE could disrupt operations, ground flights, or endanger passenger safety.

•911 and emergency dispatch – Vulnerabilities in computer-aided dispatch systems or VoIP infrastructure could delay first responders or knock out communication systems during crises. Every second lost due to a preventable system failure could cost lives.

•Banking and financial services – Financial institutions use CVEs to protect customer data and financial infrastructure. A delay in addressing a CVE affecting ATM networks or online banking platforms could result in widespread fraud, outages, or service interruptions.

"When these systems are vulnerable, lives are at risk," Santill said. "We're not just talking about data breaches—we're talking about delayed emergency response, poisoned water, power outages, and shut-down hospitals. Without the CVE program, our ability to respond to threats in these sectors falls apart."

Why the Private Sector Can’t Just ‘Foot the Bill’

Some have proposed that billion-dollar security vendors simply fund the program, but Santill cautions against this.

“Neutrality is everything,” he said. “If CVE becomes controlled by vendors, we lose trust. And MITRE, as a Federally Funded Research and Development Center (FFRDC), isn’t allowed to just accept private money to operate a public-good program like this.”

Call for Congressional Action

With no time left for contingency planning, Santill is calling on Congress to act swiftly through emergency appropriations.

“The cybersecurity community is unified on this: CVE is not optional. It’s foundational,” said Santill. “Congress must act now to protect national security, economic stability, and public safety.”

About Matt Santill:
Matt Santill is a cybersecurity expert, original contributor to the NIST Cybersecurity Framework, and founder of Cyber Security Services. He has served as Chief Information Security Officer (CISO) for the City of Santa Monica, several U.S. banks, and security leader for both public and private sector organizations. As an ethical hacker, he has tested and secured systems for hundreds of organizations, including members of the Fortune 100. He is the President of Cyber Security Services, a company based in Columbus, Ohio.

Alison Dubsky
Cyber Security Services
+1 800-390-1053
Alison.dubsky@cybersecurityservices.com
Visit us on social media:
LinkedIn