The CVE Defunding Scare: Implications for Singapore and ASEAN

by
Asha Hemrajani *and*
Davis Zheng

In April 2025, the Trump administration sparked alarm across the cybersecurity community worldwide when it announced that funding would cease for the global registry called the Common Vulnerabilities and Exposures (CVE) programme that is managed by the MITRE Corporation.

Cybersecurity vulnerabilities are flaws in computer systems that can be exploited for malicious purposes, reaping millions of dollars on the dark web.

Although the US government reversed the decision soon afterwards, the scare exposed the danger of global dependence on a single registry and raised concerns amid shifting geopolitical tensions.

The episode also reflected a broader pattern of declining US support for shared cybersecurity infrastructure following the expiry of US federal cyber threat–sharing laws and funding cuts to national coordination bodies.

The Issue at Hand

The MITRE Corporation is a non-profit entity that operates R&D centres for the US government, covering areas such as cybersecurity, homeland security, aviation and defence. Its CVE programme is a critical resource used worldwide by government agencies, armed forces, critical infrastructure operators and private enterprises to keep track of new vulnerabilities discovered in software, firmware and hardware, ranging from the Windows operating system to 5G telecommunications networks, and to patch flaws in their systems.

Vulnerability researchers submit proof of vulnerability to MITRE directly or to one of the CVE Numbering Authorities (CNAs) around the world, which include the Cyber Security Agency of Singapore. The CVE programme is available online for anyone to use, enabling IT systems administrators, for instance, to quickly act on severe vulnerabilities that may be present in their environment before threat actors can exploit them and siphon off data or, worse still, bring critical or enterprise systems to a halt.

Recent research warns that with automation today, notably with the use of AI, security flaws can be exploited with such speed that the time between the disclosure of a CVE and its weaponisation could be drastically shortened. Adversaries can now use AI systems to scan, test and exploit new vulnerabilities in mere hours. This trend magnifies the consequences of instability or underfunding in repositories such as MITRE's CVE list.

The significance of the CVE programme has been heightened following recent campaigns by threat actors such as UNC3886, the China-linked cyber espionage group that tried to attack critical infrastructure in Singapore and countries in North America, Southeast Asia and Oceania. UNC3886 is known to exploit vulnerabilities across typical enterprise computer platforms such as VMware and Fortinet to conduct malicious acts, ranging from deploying backdoors to obtaining credentials for deeper access – acts that underscore how quickly cyber defenders must act.

Other incident-sharing gaps have begun to emerge in the United States. The lapse of the federal cyber threat–sharing law during the current US government shutdown means that agencies have temporarily lost a legal framework to exchange attack data across sectors. Another example is the end of US federal government support for the Multi-State Information Sharing and Analysis Center (MS-ISAC), a non-profit centre for sharing cyber threat intelligence among US state and local governments. This decision will strain local and state capabilities to sustain shared vulnerability awareness.

The CVE system is arguably one of the most critical pillars of cybersecurity, even though it is much underrated. Not having this list to refer to is akin to not having access to a list of unique identifiers, such as the registration numbers of vehicles. Law enforcement

and traffic police would not be able to keep track of vehicles in the absence of a registry, and drivers can take advantage of the fact. For enterprises, government agencies and critical infrastructure operators, the risk of losing confidentiality, integrity and the availability of their systems could increase.

By allowing any organisation to access the registry of publicly disclosed cybersecurity vulnerabilities at no cost, the CVE programme removes information asymmetry (where one party possesses more or better information than another in a transaction), thereby improving the overall cybersecurity defence of not just the United States but of the world at large.

The Way Forward

President Donald Trump's broad strokes federal cost-cutting efforts have resulted in funding uncertainty for programmes such as the CVE. Had the Trump administration failed to reverse its initial defunding decision, it would have had dangerous implications for every organisation that utilises the CVE programme. Organisations without their own vulnerability research capabilities would have been at risk since vulnerabilities found would have had no way of being disclosed publicly.

Several ideas to keep the CVE list going have been suggested. Some believe that the list should not come under the purview of a single government but rather a global organisation, such as the United Nations, and managed by multiple countries. However, this is unlikely to work well as the CVE programme is a multistakeholder undertaking that relies heavily on commercial enterprises and private individuals to contribute their research, rather than on governments alone.

Another suggestion is for the registry to come under the purview of the Internet Engineering Task Force (IETF), a global organisation for internet standards, protocols and operations. However, parking the programme under another non-profit international organisation has disadvantages, such as cost and administration.

Meanwhile, the European Union has taken matters into its own hands. The EU Vulnerability Database (EUVD) was launched in May 2025 by the European Union Agency for Cybersecurity (ENISA) to reduce its reliance on the MITRE CVE programme. It is designed to be a publicly accessible database. It is part of the European Union's effort to strengthen its cybersecurity sovereignty and reduce reliance on external threat intelligence ecosystems.

Implications for Singapore and ASEAN

The volatility of US government support for cybersecurity functions underscores the need for the rest of the world to develop regional cyber resilience capabilities of their own.

Due to Singapore's small size, it is unlikely that the country can develop the capability to create its own comprehensive database with sufficient data to be useful solely based on its national vulnerability research output. Singapore would still have to rely heavily on international databases such as ENISA's EUVD and the US CVE programme to supplement its own defences.

A possible alternative measure for ASEAN would be to adopt a decentralised model to create redundancy. Singapore could be one of several countries that host or maintain a cooperative decentralised database, similar to the EUVD, mirrored across ASEAN partner countries, ensuring constant uptime and reducing the maintenance burden on participating nations. Such an approach would allow for confidence-building measures and capability development among ASEAN member states.

Given that funding for the US MITRE CVE database has only been committed until March 2026, the future of the database has been left hanging. Even if funding is renewed, the situation must be monitored closely. Singapore should explore alternative solutions to the MITRE CVE as it is a critical resource for the nation's cybersecurity needs.

This essay was first published in RSIS Commentary.

Asha Hemrajani and Davis Zheng are, respectively, Senior Fellow and Research Assistant in the Centre of Excellence for National Security (CENS), at RSIS.