RSIS COMMENTARY

22 September 2025

The CVE Funding Crisis: Implications for Singapore and ASEAN

Asha Hemrajani and Davis Zheng

RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ponder the Improbable since 1996

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 194 – 22 September 2025

The CVE Funding Crisis: Implications for Singapore and ASEAN

By Asha Hemrajani and Davis Zheng

SYNOPSIS

In April 2025, the US-funded MITRE Corporation, which manages a registry (called the Common Vulnerabilities and Exposures (CVE) programme) of cybersecurity vulnerabilities – flaws in computer systems – that can be exploited for malicious purposes, announced that the funding for the CVE programme would cease, sparking alarm across the cybersecurity community. Although the US government reversed the decision, the scare exposed the danger of global dependence on a single registry and raised concerns amid shifting geopolitical tensions.

COMMENTARY

Cybersecurity vulnerabilities are flaws in computer systems that can be exploited for malicious purposes and are often worth millions of dollars on the dark web. The MITRE Corporation manages the global registry of such flaws. Called the Common Vulnerabilities and Exposures (CVE) programme, it is a critical resource used by governments and enterprises globally to patch flaws in their systems.

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

Vulnerability researchers submit proof of vulnerability to MITRE directly or to one of the CVE Numbering Authorities (CNAs) around the world, which includes the Cyber Security Agency of Singapore. This registry of cybersecurity vulnerabilities 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.

The significance of the CVE programme has been heightened following recent campaigns by actors such as UNC3886, the China-linked cyber espionage group that tried to attack critical infrastructure in Singapore and other 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 actions, ranging from deploying backdoors to obtaining credentials for deeper access, which underscores how quickly cyber defenders must act.

The CVE system is arguably one of the most critical pillars of cybersecurity, even though it is much underrated. Without this list to refer to is akin to not having access to a list of unique identifiers, such as, for example, the registration numbers of vehicles. Law enforcement and traffic police would not be able to keep track of vehicles, 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.

The CVE programme allows any organisation to access the registry of publicly disclosed cybersecurity vulnerabilities without any cost, and 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 that of the world.

The Issue at Hand

President Donald Trump's broad strokes in cutting federal funding have resulted in a funding crisis for programmes such as the CVE. The possible loss of the programme has dangerous implications for every organisation that utilises it. It would result in a decreased security posture as organisations without their own vulnerability research capabilities would be at risk, since vulnerabilities found would have no way of being disclosed publicly.

The European Union has taken matters into its own hands. The EU Vulnerability Database (EUVD) is a recent initiative launched 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. This is part of the EU's effort to strengthen its cybersecurity sovereignty and reduce reliance on external threat intelligence ecosystems.

The Way Forward

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 UN 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.

Another suggestion is for the registry to come under the purview of the *Internet Engineering Task Force* (IETF), which is 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.

Implications for Singapore and ASEAN

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.

An alternative measure for Singapore would be to adopt a decentralised model to create redundancy. Singapore can be one of the countries that hosts or maintains a decentralised database, which is mirrored across partner countries such as ASEAN, ensuring constant uptime and reducing the maintenance burden on participating nations. This would allow for possible confidence-building measures and capability development amongst 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.

Asha Hemrajani and Davis Zheng are, respectively, Senior Fellow and Research Assistant in the Centre of Excellence for National Security (CENS), at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU).