MeriTalk
Improving the Outcomes of Government IT

Sen. Warner Says DoD Must Strengthen Cyber Vulnerability Disclosure Programs

NEWS EMERGING TECH CYBERSECURITY Feb 27, 2020 | 12:05 pm

SHARE THIS STORY

In a Feb. 26 letter to Dana Deasy, CIO of the Department of Defense (DoD), Sen. Mark Warner, D-Va., stressed the importance of vulnerability disclosure programs.

Warner's letter followed news of malware on the DoD webserver. The malware was actively exploiting a security misconfiguration and was only brought to light when a researcher used a vulnerability disclosure program to report the malware. Warner, who is the vice chairman of the Senate Select Committee on Intelligence and co-chair of the Senate Cybersecurity Caucus, noted that according to current reporting, the malware was part of a botnet that mine cryptocurrency using DoD resources and IT systems. The incident "raises broader cybersecurity concerns," he said.

"This incident demonstrates the inherent

CATEGORIES

Recent

Navy IT and the New "Employee Bathroom Test"

RSA Live: GM CEO Says Security Central to Autonomous Vision

Coast Guard Wants Tech for Maritime Tracking

JAIC Hires Alka Patel to Lead AI Ethics

Global Cybersecurity Norms are at a Crossroads, Report Says

value of vulnerability disclosure programs for information technology products operated by Federal agencies," wrote Warner. "These programs are a crucial force multiplier for Federal cybersecurity efforts. Clear guidelines and a process for security researchers to find and share vulnerabilities enabled this malware discovery, and ultimately prompt remedial action by DoD. Continuing to encourage the responsible discovery and disclosure of bugs or vulnerabilities on Federal information technology systems with both internal and outside security researchers can only strengthen the cybersecurity posture of Federal and DoD systems."

In his letter, Warner highlighted the Internet of Things Cybersecurity Improvement Act. The legislation, which he sponsored, "would help advance similar coordinated vulnerability programs and work in conjunction with the procedures in place at DoD," Warner explained. He also addressed the importance of adequate cybersecurity protections, specifically on commercial cloud-computing platforms and open source software.

"While the use of commercial cloud computing can be a cost effective method to deploy and manage information technology and services, the use of a cloud itself does not ensure cybersecurity," he said. "Rigorous cybersecurity defensive measures and monitoring remain crucial for systems, even when DoD resources are deployed on commercial cloud computing platforms. While open source software, such as the automation server employed in this incident, may be beneficial, it is also essential to monitor all software for vulnerabilities and ensure they are promptly mitigated. Likewise, continuous use of software requires an effective continuous monitoring process for addressing newly discovered vulnerabilities in the software. And perhaps most importantly in the shared security model of commercial cloud computing, ensuring safe and secure configurations related to access is a key concern."

He concluded by saying that he was hopeful the DoD will "take the lessons from this incident seriously and reassess current processes as necessary."

SHARE THIS STORY

TAGS: DANA DEASY, MARK WARNER

HOME NEWS INSIGHT EXCHANGES EVENTS RESEARCH AWARDS
ABOUT | AFFILIATES | ADVERTISE | CONTACT | TERMS OF USE