Log4j software flaw 'endemic,' new cyber safety panel says

July 14 2022, by ALAN SUDERMAN

The Department of Homeland Security logo is seen during a news conference in Washington, Feb. 25, 2015. A new cybersecurity panel created by President Joe Biden says a computer vulnerability discovered last year in a ubiquitous piece of software is an "endemic" problem that will pose security risks for potentially a decade or more. The Cyber Safety Review Board said in a new report Thursday that while there hasn't been sign of any major cyberattack due to the Log4j flaw, it will still "be exploited for years to come." The Log4j flaw was first made public late last year. Credit: AP Photo/Pablo Martinez Monsivais, File

A computer vulnerability discovered last year in a ubiquitous piece of software is an "endemic" problem that will pose security risks for potentially a decade or more, according to a new cybersecurity panel created by President Joe Biden.

The Cyber Safety Review Board said in a report Thursday that while there hasn't been sign of any major cyberattack due to the Log4j flaw, it will still "be exploited for years to come."

"Log4j is one of the most serious software vulnerabilities in history," the board's chairman, Department of Homeland Security Under Secretary Rob Silvers, told reporters Wednesday.

The Log4j flaw, made public late last year, lets internet-based attackers easily seize control of everything from industrial control systems to web servers and consumer electronics. The first obvious signs of the flaw's exploitation appeared in Minecraft, a hugely popular online game owned by Microsoft.

The flaw's discovery prompted urgent warnings by government officials and massive efforts by cybersecurity professionals to patch vulnerable systems.

The board said Thursday that "somewhat surprisingly" the exploitation of the Log4j bug had occurred at lower levels than experts predicted. The board also said that it was unaware of any "significant" Log4j attacks on critical infrastructure systems but noted that some cyberattacks go unreported.

The board said future attacks are likely in large part because Log4j is routinely embedded with other software and can be hard for

organizations to find running in their systems.

"This event is not over," Silvers said.

Log4j, written in the Java programming language, logs user activity on computers. Developed and maintained by a handful of volunteers under the auspices of the open-source Apache Software Foundation, it is extremely popular with commercial software developers.

A security researcher at the Chinese tech giant Alibaba notified the foundation on Nov. 24. It took two weeks to develop and release a fix. Chinese media reported that the government punished Alibaba for not reporting the flaw earlier to state officials.

The board said Thursday it found "troubling elements" with the Chinese government's policy toward vulnerability disclosures, saying it could give Chinese state hackers an early look at computer flaws they could use for nefarious means like stealing trade secrets or spying on dissidents. The Chinese government has long denied wrongdoing in cyberspace and told the board that it encourages improved information sharing on software vulnerabilities.

The board offered a number of recommendations on mitigating the fallout of the Log4j flaw as well as improving cybersecurity generally. That includes the suggestion that universities and community colleges make cybersecurity training a required part of computer science degree and certification programs.

The Cyber Safety Review Board is modeled after the National Transportation Safety Board, which reviews plane crashes and other major accidents, and was mandated by an executive order Biden signed last May. The 15-member board is made up of FBI, National Security Agency and other government officials as well as people from the

private sector. Some supporters of the new board criticized DHS for taking so long to get it up and running.

Biden's executive order directed the board to conduct its first review on the massive Russian cyber espionage campaign known as SolarWinds. Russian hackers were able to breach several federal agencies, including accounts belonging to top cybersecurity officials at DHS, though the full fallout from that campaign is still unclear.

Silvers said DHS and the White House agreed that reviewing the Log4j flaw was a better use of the new board's expertise and time.