THE HILL

Government software may have let in foreign spies

Getty Images

By Cory Bennett and Katie Bo Williams - 02/02/16 06:00 AM EST

The government may have used compromised software for up to three years, exposing national security secrets to foreign spies, according to lawmakers and security experts.

Observers increasingly believe the software defect derived from an encryption “back door” created by the National Security Agency (NSA). Foreign hackers likely repurposed it for their own snooping needs.

The House Oversight Committee has launched an investigation into the matter, but specialists and former government officials say confidentiality concerns might prevent the public from ever knowing if a breach occurred.

“There’s a lot of very sketchy stuff here,” said Matthew Green, a cryptology expert from Johns Hopkins University who has been reverse-engineering the compromised code.

The software vulnerability was spotted in December, when Juniper Networks, which makes a variety of IT products widely used in government, said it had found unauthorized code in its ScreenOS product.

Security experts said the code had been intentionally altered, and Juniper acknowledged that the alteration could let hackers infiltrate networks and decrypt traffic.

One U.S. official compared the alteration to “stealing a master key to get into any government building,” according to CNN.

“It’s a very serious problem,” said Sen. **Ron Johnson** (R-Wis.), who heads the Senate Homeland Security and Governmental Affairs Committee. “It affects everybody’s IT systems.”

The software flaw may have affected agencies ranging from the Defense Department to the Department of Health and Human Services to the State Department and the Office of Personnel Management, which suffered its own extensive hacks this past year.

Researchers say a foreign government is likely behind the defect. The ability to turn the Juniper code into a usable back door required not only sophisticated hacking abilities but also the infrastructure to eavesdrop on the encrypted traffic.

“Very few people outside of nation states have both of those things,” Green said.

Juniper has relied on the vulnerable piece of code since at least 2013, meaning that foreign adversaries might have had years to pilfer national security secrets and plant the seeds of future cyberattacks.

“Once adversaries get into a network, they’re often able to move laterally,” said Paul Stockton, the assistant secretary of Defense for homeland defense from 2009 to 2013.

Once inside a network, hackers can pick up passwords, map networks and gain knowledge that could “provide for trapdoor access to be able to get back in at times of their own choosing,” Stockton added.

The case is especially frustrating to security experts because it may have been avoidable. The hackers, they say, likely benefited from a flaw in the encryption algorithm that was inserted by the NSA.

For years, the NSA was seen as the standard-bearer on security technology, with many companies relying on the agency’s algorithms to lock down data.

But some suspected the NSA algorithms, including the one Juniper used, contained built-in vulnerabilities that could be used for surveillance purposes. Documents leaked by former NSA contractor Edward Snowden in 2013 appeared to confirm those suspicions.

“That pretty solidly pointed the finger at these algorithms having been tampered with or made vulnerable by the NSA,” Green said.

Juniper has since said it will no longer rely on that NSA-developed encryption algorithm to secure ScreenOS, another blow to the NSA’s position as a leader on encryption standards.

The issue has also sparked the attention of some tech-savvy lawmakers.

The Oversight Committee is primarily concerned that federal agencies haven’t applied the patch that Juniper offers to close the back door.

Government agencies are scanning their networks to see what may have been compromised, but the months-long process has frustrated lawmakers.

Officials are “dragging their feet,” said Rep. Will Hurd (R-Texas), who chairs the Oversight Committee’s subpanel on information technology.

“If government systems have yet to be fixed, then adversaries could still be stealing sensitive information crucial to national security,” Hurd wrote in a Wall Street Journal op-ed. “The Department of Homeland Security is furiously working to determine the extent to which the federal government used ScreenOS. But Congress still doesn’t know the basic details of the breach.”

Many in Congress haven’t even heard about the Juniper Networks flaw. Several intelligence and homeland security leaders in both parties told The Hill the issue was not yet on their radar, but that appears likely to change.

Federal agencies were given a Feb. 4 deadline for responding to the Oversight Committee’s inquiries about the Juniper software patch. After those responses are received, committee leaders will determine whether they can hold open hearings on the matter.

“This is certainly something that we’ve got to be aware of and see what comes to light,” Johnson said, adding that his Senate committee could follow up with its own investigation or hearings.

But congressional pressure can’t overcome the inherent difficulties of tracing a hack to its source.

Advanced hackers are adept enough to “hide their tracks and to clean up after themselves,” said Stockton, now the managing director of consultancy Sonecon LLC.

That means the Juniper defect could provide foreign hackers with an undetectable “persistent presence” in government networks, Stockton said.

“We don’t know yet.”

TAGS: Ron Johnson

The Hill 1625 K Street, NW Suite 900 Washington DC 20006 | 202-628-8500 tel | 202-628-8503 fax