Technology | Sat Jan 9, 2016 1:53pm EST Related: TECH

Juniper Networks will drop code tied to National Security Agency

SAN FRANCISCO | BY JOSEPH MENN

A National Security Agency (NSA) data gathering facility is seen in Bluffdale, about 25 miles (40 km) south of Salt Lake City, Utah, December 16, 2013. Jim Urquhart/
REUTERS

Juniper Networks Inc said late on Friday it would stop using a piece of security code that analysts believe was developed by the National Security Agency in order to eavesdrop through technology products.

The Silicon Valley maker of networking gear said it would ship new versions of security software in the first half of this year to replace those that rely on numbers generated by Dual Elliptic Curve technology.

The statement on a blog post came a day after the presentation at a Stanford University conference of research by a team of cryptographers who found that Juniper's code had been changed in multiple ways during 2008 to enable eavesdropping on virtual private network sessions by customers.

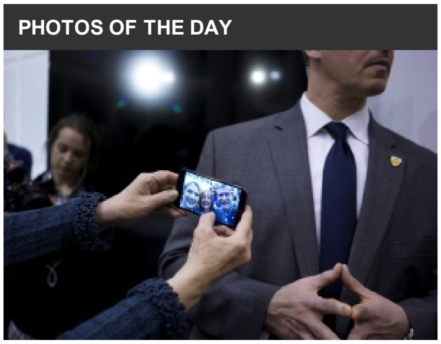
Last month, Sunnyvale-based Juniper said it had found and replaced two unauthorized pieces of code that allowed "back door" access, which the researchers said had appeared in 2012 and 2014.

EDITOR'S CHOICE

Hope, frustration for Iranians after sanctions lifted

In Atlantic City: pride, anger, worry

PHOTOS OF THE DAY



Our top photos from the last 24 hours. Slideshow »

Battle for Iowa

El Nino claims California apartment

The 2014 back door was straightforward, said researcher Hovav Shacham of the University of California, San Diego, allowing anyone with the right password to see everything.

The 2012 code changed a mathematical constant in Juniper's Netscreen products that should have allowed its author to eavesdrop, according to Shacham and his fellow investigators.

Juniper's initial patch had gotten rid of that constant in Dual Elliptic Curve and replaced it with the version it had been using since 2008.

But the academics who studied the code said that while Juniper had not disavowed the 2008 code, it had not explained how that constant was picked or why it was using the widely faulted Dual Elliptic Curve at all.

Still another curve constant, quietly provided by the NSA and required for some federal certification, was exposed in documents leaked by former NSA contractor Edward Snowden as a key to the back door.

Until now, the most influential adopter of Dual Elliptic Curve was believed to be RSA, part of storage company EMC, which Reuters reported received a $10-million federal contract to distribute it in a software kit for others.

Though the academic team looking at Juniper has not named a suspect in the 2008, 2012 or 2014 changes, 2008 was one year after veteran cryptographers raised questions about Dual Elliptic Curve.

A very advanced adversary could have seen how to manipulate Dual EC and in theory managed to insert code through a cooperative or unsuspecting Juniper employee, but the company had not advertised the fact that it was using the formula at all.

A more logical suspect, said expert Nicholas Weaver of the International Computer Science Institute, was the NSA, which might have been displaced later by other countries' agencies or top-level hackers in 2012 and 2014.

The NSA did not immediately respond to an emailed request for comment.

Juniper said it was continuing to investigate. here

It declined to answer questions from Reuters about the revisions.

(Reporting by Joseph Menn; Editing by Clarence Fernandez)

TRENDING ON REUTERS

Oregon occupation leader Bundy urges remaining protesters to go home | 1

How Planned Parenthood's accusers became the accused in Texas case 2

Fed keeps rates unchanged, wary eye on global markets | 3

Trump steps up attacks with 'bimbo' tweet before Fox News debate | 4

China shares flounder again, but 'real economy' sound says state media | 5