Juniper breach reflects risk of 'back doors': researchers

WASHINGTON | BY DUSTIN VOLZ

A Juniper Networks Inc software coding vulnerability disclosed last week shows the dangers of any weaknesses built into encryption technology, according to computer security experts.

The apparent "back door" in Juniper's routers, which direct digital traffic around the Internet, could only have been planted by a handful of governments due to its sophistication, researchers said this week.

A growing number of U.S. presidential candidates and policymakers are clamoring for access to encrypted data, arguing that secrecy in communications helps criminals conceal their plots.

Technology companies have fiercely resisted limiting the use of encryption or providing special government access, saying it is technically unfeasible and undermines customer privacy.

Democratic presidential frontrunner Hillary Clinton on Saturday called for greater collaboration between Silicon Valley and government codebreakers, as the attacks in Paris and San Bernardino, California, renewed questions about the potential use of encryption by violent extremists.
Federal officials are investigating the Juniper breach, as the U.S. government relies on the Sunnyvale, California-based company’s software in some of its networks.

It is unclear how the Juniper vulnerability was planted or by whom. The company used a cryptography standard developed and promoted by the National Security Agency.

But Microsoft Corp researchers determined in 2007 that the technology was flawed because the output of its random number generator could be predicted, enabling the system’s designers or others to break the encryption.

Many researchers believe files released by former NSA contractor Edward Snowden show the flaw was a deliberate effort by the spy agency to maintain eavesdropping capabilities. (reut.rs/1U5bnAW)

Juniper developed an alternate standard, but it was still based on the flawed one pushed by the NSA, which paved the way for the security hole announced last week.

"If this really was intended as a 'nobody but us' back door and then subverted by a nation state, that's a tricky place for policymakers," said Dave Palmer, director of technology for the cybersecurity firm Darktrace. The Juniper incident demonstrates that no back door is "absolutely bulletproof" to hackers, the former security analyst at the British spy agency GCHQ added.

"Whenever you build in access, you're running a risk ... that that access will be misused," said Stewart Baker, former general counsel at the NSA who now is a partner at Steptoe & Johnson. "The question here is, is this a risk that ought to be managed or should we refuse to accept it at all?"

(Reporting by Dustin Volz; Editing by Jonathan Weber and Richard Chang)