eWEEK® Enterprise IT Technology News, Opinion and Reviews

Juniper Networks Moves to Replace Vulnerable Code

By **Sean Michael Kerner** | Posted 2016-01-11

At the end of 2015, Juniper Networks publicly disclosed that it had found previously unknown backdoor code on some of its firewalls. Juniper patched the issues and is now going a step further by replacing a core cryptography component in its ScreenOS operating system to further reduce any potential risk.

A core element of many forms of cryptography is the use of random number generators. The ScreenOS operating system makes use of the Dual_EC DBRG (Dual Elliptic Curve Deterministic Random Bit Generator) and ANSI X9.31random number technologies. Back in 2014, reports emerged alleging that Dual_EC DBRG was intentionally weakened in order to enable the placement of a backdoor by the U.S. National Security Agency (NSA).

Bob Worrall, senior vice president and CIO of Juniper Networks, is now moving to have his company remove Dual_EC DBRG from ScreenOS entirely.

With the initial patch for ScreenOS that protects users against backdoor code, Dual_EC remains in place.

"We remain confident that the patched releases, which use Dual_EC, remediate both the unauthorized administrative access issue, as well as the VPN decryption issue," Worrall wrote in a blog post.

ScreenOS is the core operating systems used on Juniper's Netscreen firewalls, which have largely been superseded in the company's product portfolio in recent years by the SRX Firewall product portfolio. The SRX runs on Juniper's Junos operating system, which is the same operating system that powers most of the company's switches and routers.

After the initial discovery of the backdoor code on ScreenOS, Worrall commented that Juniper started a comprehensive investigation into both ScreenOS and Junos source code. The end result of that investigation is that there is no evidence to suggest any unathorized code or backdoor in Junos.

"The investigation also confirmed that it would be much more difficult to insert the same type of unauthorized code in Junos OS," Worrall said.

One reason it would be more difficult to insert unauthorized backdoor code in Junos that it uses a different random number generation system. To that end, Juniper is going to replace Dual_EC in ScreenOS 6.3 and instead make use of Junos' random number generation technology. The change is expected to land in a ScreenOS update that is set to become available in the first half of the year.

Itay Glick, CEO of security specialist Votiro, is not surprised that Juniper is replacing the DUAL_EC component and suggested that other vendors do the same and move to a well-validated algorithm.

"Every company that uses compromised components should strive not to use them," Glick told *eWEEK*.

Areg Alimian, senior director of solutions marketing at security specialist Ixia, is also not surprised that Juniper is moving to replace potentially vulnerable cryptography components in its software. A key lesson that can be learned from this incident is that entropy needs to be more automatic and easier to add into security systems, he said.

"Random number generators (RNG) are essential but can't be the lynchpin to any system," Alimian told *eWEEK*.

Sean Michael Kerner is a senior editor at eWEEK *and* InternetNews.com*. Follow him on Twitter @TechJournalist*.