Juniper Networks to NetScreen users: Patch now

December 18 2015, by Nancy Owano

Juniper Networks said unauthorized code was discovered in ScreenOS, reported Simon Sharwood in *The Register* on Thursday. This is the operating system for its NetScreen firewalls. An attacker with that code may achieve administrative access to NetScreen devices— and decrypt VPN connections.

"Firewalls are rich targets for cyberattackers since the devices monitor all data traffic flowing in and out of an organization," said Jeremey Kirk, IDG News Service.

Kirk wrote that one of the vulnerabilities could allow an attacker to monitor VPN traffic to decrypt it. "VPNs are encrypted connections between a user and another computer and are often used by companies to allow secure remote access to their systems for employees who are traveling."

Who does this apply to? Juniper said that all NetScreen devices using ScreenOS 6.2.0r15 through 6.2.0r18 and 6.3.0r12 through 6.3.0r20 are affected by these issues and require patching.

Juniper, said Sharwood, issued a patch for the problem and the company strongly advised on its application as soon as possible. (The company said, "we strongly recommend that customers update their systems and apply the patched releases with the highest priority.")

Juniper on Thursday issued this with the header of "Important Juniper Security Announcement," authored by Bob Worrall, SVP chief information officer.

He said that Juniper "wanted to make customers aware of critical patched releases we are issuing today to address vulnerabilities in devices running ScreenOS software."

He said Juniper discovered the code during a recent internal code review. Once identified, the company launched an investigation and developed patched releases for the latest versions of ScreenOS.

For those applying the update to systems, Worrall said more information was available in the Juniper Security Advisories on the company's Security Incident Response website. Dan Goodin, Security Editor at *Ars Technica*, noted there was no evidence right now that the backdoor was put in other Juniper OSes or devices.

Responding to the question if the SRX or other Junos-based system was affected, Juniper said the vulnerabilities were specific to ScreenOS. "We have no evidence that the SRX or other devices running Junos are impacted at this time."

"It's not clear how the code got there," said Goodin on Thursday; Juniper's advisory did not mention who it suspected.

Tim Greene, who covers security for *Network World*, addressed the question if any other Juniper gear was affected. According to Greene, Juniper said there was no evidence it is.

The company site states that "the world's top 100 service providers—the biggest and busiest wireline and wireless carriers, cable and satellite operators, content and Internet services providers, and cloud and data center providers—run on Juniper Networks. So do major banks and other global financial services organizations, seven of the eight largest stock exchanges in the world, national government agencies and U.S. federal organizations, healthcare and educational institutions, energy and utility companies, and 99 of the Fortune Global 100."

More information: forums.juniper.net/t5/Security … ScreenOS/ba-p/285554