The Intercept_

NSA HELPED BRITISH SPIES FIND SECURITY HOLES IN JUNIPER FIREWALLS

Ryan Gallagher, Glenn Greenwald

Dec. 23 2015, 12:25 p.m.

90

Photo: Simon Dawson/Bloomberg/Getty Images

A TOP-SECRET document dated February 2011 reveals that British spy agency GCHQ, with the knowledge and apparent cooperation of the NSA, acquired the capability to covertly exploit security vulnerabilities in 13 different models of firewalls made by Juniper Networks, a leading provider of networking and Internet security

gear.

The six-page document, titled "Assessment of Intelligence Opportunity – Juniper," raises questions about whether the intelligence agencies were responsible for or culpable in the creation of security holes disclosed by Juniper last week. While it does not establish a certain link between GCHQ, NSA, and the Juniper hacks, it does make clear that, like the unidentified parties behind those hacks, the agencies found ways to penetrate the "NetScreen" line of security products, which help companies create online firewalls and virtual private networks, or VPNs. It further indicates that, also like the hackers, GCHQ's capabilities clustered around an operating system called "ScreenOS," which powers only a subset of products sold by Juniper, including the NetScreen line. Juniper's other products, which include high-volume Internet routers, run a different operating system called JUNOS.

The possibility of links between the security holes and the intelligence agencies is particularly important given an ongoing debate in the U.S. and the U.K. over whether governments should have backdoors allowing access to encrypted data. Cryptographers and security researchers have raised the possibility that one of the newly discovered Juniper vulnerabilities stemmed from an encryption backdoor engineered by the NSA and co-opted by someone else. Meanwhile, U.S. officials are reviewing how the Juniper hacks could affect their own networks, putting them in the awkward position of scrambling to shore up their own encryption even as they criticize the growing use of encryption by others.

The headquarters of Juniper Networks in Sunnyvale, Calif., on Jan. 1, 2014. Photo: Kris Tripplaar/Sipa USA/AP

The author of the 2011 GCHQ document, an NSA employee who was working with GCHQ as part of an "Access Strategy Team," takes a similarly adversarial view of encryption, referring to Juniper as a "threat" and a "target" because it provides technology to protect data from eavesdropping. Far from suggesting that security agencies should help U.S. and U.K. companies mend their digital defenses, the document says the agencies must "keep up with Juniper technology" in the pursuit of SIGINT, or signals intelligence.

"The threat comes from Juniper's investment and emphasis on being a security leader," the document says. "If the SIGINT community falls behind, it might take years to regain a Juniper firewall or router access capability if Juniper continues to rapidly increase their security."

The document, provided by NSA whistleblower Edward Snowden, shines light on the agencies' secret efforts to ensure they could monitor information as it flowed through Juniper's products, which are used by Internet providers, banks, universities, and government agencies. It notes that while Juniper trails its competitors, it is a "technology leader" with gear "at the core of the Internet in many countries," including several deemed to be high priority from a spying perspective: Pakistan, Yemen, and China.

[redacted] "Juniper technology sharing with NSA improved dramatically to exploit several target networks"

Asked about the document, GCHQ issued a boilerplate response asserting that the agency does not comment on intelligence matters and complies with "a strict legal and policy framework." The NSA could not immediately respond Tuesday. Juniper sent a written statement saying the company "operates with the highest of ethical standards, and is committed to maintaining the integrity, security, and quality of our products. As we've stated previously … it is against established Juniper policy to intentionally include 'backdoors' that would potentially compromise our products or put our customers at risk. Moreover, it is Juniper policy not to work with others to introduce vulnerabilities into our products."

Juniper's prominence and ubiquity similarly helped draw attention to the more recent hacks against the company, which first came to light Thursday, when the California firm revealed it had discovered "unauthorized code" in ScreenOS enabling two major vulnerabilities. One, first present in an August 2012 release of ScreenOS, could allow access to encrypted data transmitted over VPNs. The other, first surfacing in a December 2014 ScreenOS release, allows an attacker to remotely administer a firewall, thus

leading to "complete compromise of the affected device," according to Juniper. The vulnerabilities remained in versions of ScreenOS released through at least October of this year.

It is the earlier vulnerability, potentially allowing eavesdropping on VPNs, that has generated vigorous online discussion among computer security experts. Some, like Johns Hopkins professor Matthew Green and security researcher Ralf-Philipp Weinmann, have said that an attacker appears to have subverted a backdoor shown, in previously disclosed documents from Snowden, to have originated with the NSA. Specifically, the attacker seems to have tampered with a 32-byte value used to seed the generation of random numbers, numbers that are in turn used in the process of encrypting data in ScreenOS. ScreenOS uses the value as a parameter to a standard system for random number generation known as Dual Elliptic Curve Deterministic Random Bit Generator. The default 32-byte value in this standard is believed to have been generated by the NSA. Juniper said, in the wake of the Snowden revelations about the standard, that it had replaced this 32-byte value with its own "self-generated basis points." So the attacker would have replaced Juniper's replacement of the NSA 32-byte value.

Matt Blaze, a cryptographic researcher and director of the Distributed Systems Lab at the University of Pennsylvania, said the document contains clues that indicate the 2011 capabilities against Juniper are not connected to the recently discovered vulnerabilities. The 2011 assessment notes that "some reverse engineering may be required depending on firmware revisions" affecting targeted NetScreen firewall models. Blaze said this points away from the sort of ScreenOS compromise behind the more

recent Juniper vulnerabilities.

"With the [recently discovered] backdoor, a firmware revision would either have the backdoor or it wouldn't, and if it was removed, they'd have to do a lot more than 'some reverse engineering' to recover the capability," Blaze said. "My guess from reading this is that the capabilities discussed here involved exploiting bugs and maybe supply chain attacks, rather than this [recently discovered] backdoor."

Blaze said the exploit capabilities in the 2011 document seem consistent with a program called "FEEDTROUGH," first revealed in a 2007 document published alongside an article in German newsweekly *Der Spiegel*.

Even if it outlines capabilities unconnected to the recently discovered Juniper hacks, the 2011 GCHQ assessment makes clear that the author was interested in expanding the agencies' capabilities against Juniper. "The vast majority of current Juniper exploits are against firewalls running the ScreenOS operating system," the author wrote. "An effort to ensure exploitation capability" against Juniper's primary operating system, JUNOS, "should bear fruit against a wide range of Juniper products."

The document suggests that the intelligence agencies successfully used the security holes they identified in Juniper's devices to repeatedly penetrate them for surveillance, stating that "Juniper technology sharing with NSA improved dramatically during [calendar year] 2010 to exploit several target networks where GCHQ had access primacy."

The assessment also notes that, because Juniper is a U.S.-based

company, there is both “opportunity and complication” in targeting its technology. “There is potential to leverage a corporate relationship should one exist with NSA,” it says, adding: “Any GCHQ efforts to exploit Juniper must begin with close coordination with NSA.”

It further states that GCHQ has a “current exploit capability” against 13 Juniper models, all of which run ScreenOS: NS5gt, N25, NS50, NS500, NS204, NS208, NS5200, NS5000, SSG5, SSG20, SSG140, ISG 1000, ISG 2000. It reveals that the agency was developing an additional surveillance capability to hack into high-capacity Juniper M320 routers, which were designed to be used by Internet service providers.

“The ability to exploit Juniper servers and firewalls,” the document says, “will pay many dividends over the years.”

TOP SECRET STRAP1
ASSESSMENT OF INTELLIGENCE OPPORTUNITY - JUNIPER

03 February 2011

Executive Summary

Background

- Juniper Networks, Inc. headquartered in Sunnyvale, California, USA is a high-performance Internet Protocol network products company. Juniper's main products include *T-series*, *M-series*, *E-series*, *MX-series*, and *J-series* families of routers, *EX-series* Ethernet switches, and NetScreen and SRX-series security products.
- While Juniper is not necessarily the market share leader in any one space, they are a strong competitor and technology leader across several important markets from a SIGINT perspective. Juniper is at the core of the Internet in many countries by virtue of providing the highest density routers for many years.
- Juniper's leadership in core IP routing and the Enterprise Network Firewall and SSL VPN markets means that the SIGINT community should keep up with Juniper technology to be [illegible] to maintain CNE access over time.

Juniper-Opportunity-Assessment-03FEB11-Redacted
7 pages

[illegible] Juniper NetScreen Firewalls models NS5gt, N25, NS50, NS500, NS204, NS208, NS5200, NS5000, SSG5, SSG20, SSG140, ISG 1000, ISG 2000. Some reverse engineering may be required depending on firmware revisions.

CONTACT THE AUTHOR:

Ryan Gallagher
ryan.gallagher@theintercept.com
@rj_gallagher

Glenn Greenwald
glenn.greenwald@theintercept.com
@ggreenwald

90 Comments (closed)

The Intercept_

HARROWING TREATMENT OF YEMENI-AMERICANS DEMANDS GOVERNMENT PROBE, GROUPS SAY

Smitha Khorana

Jan. 27 2016, 4:11 p.m.

3

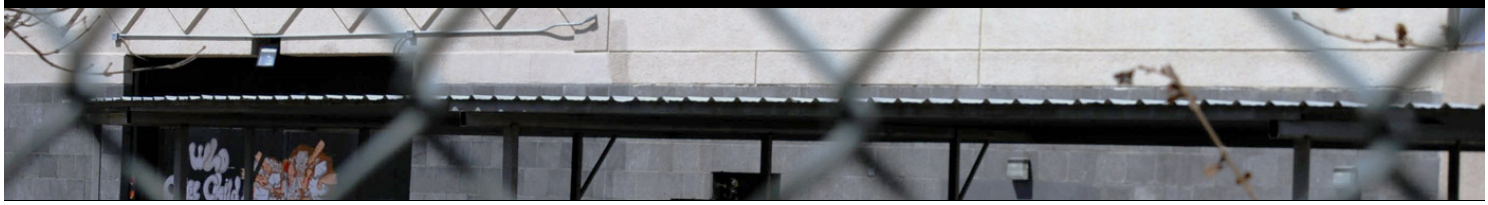

Photo: Mohammed Hamoud/Anadolu Agency/Getty Images

CIVIL LIBERTIES GROUPS have asked the State Department's Office of Inspector General to investigate what they said were years of misconduct at the U.S. Embassy in Sanaa, including a wave of dubious passport revocations.

The request, which includes previously unreleased emails from seemingly desperate Americans stranded in Yemen, comes as seven civil rights and immigration lawyers from across the U.S. tell *The Intercept* that their clients have had their passports revoked without due process, resulting in them being separated from their children, fired from jobs, placed under suspicion, singled out for treatment not inflicted on other immigrant groups, and told to remain silent about their ordeals, among other travails.

The report to the State Department paints a similarly harrowing picture of the treatment of Yemeni-Americans who had passports confiscated. Submitted yesterday by Asian Americans Advancing

Justice — Asian Law Caucus and CLEAR, a free legal clinic at the City University of New York School of Law, it details instances of coercive interrogations and of U.S. citizens stranded in Yemen and separated from family members for years. Although many were eventually allowed to fly back to the U.S., they continue to face various restrictions on their travel.

The report says the Yemeni-Americans were coerced into signing confessions that fraudulent names were used in their

Read more

ASSESSMENT OF INTELLIGENCE OPPORTUNITY - JUNIPER

03 February 2011

Executive Summary

Background

- Juniper Networks, Inc. headquartered in Sunnyvale, California, USA is a high-performance Internet Protocol network products company. Juniper's main products include *T-series*, *M-series*, *E-series*, *MX-series*, and *J-series* families of routers, *EX-series* Ethernet switches, and NetScreen and SRX-series security products.
- While Juniper is not necessarily the market share leader in any one space, they are a strong competitor and technology leader across several important markets from a SIGINT perspective. Juniper is at the core of the Internet in many countries by virtue of providing the highest density routers for many years.
- Juniper's leadership in core IP routing and the Enterprise Network Firewall and SSL VPN markets means that the SIGINT community should keep up with Juniper technology to be positioned to maintain CNE access over time.

Currently exploit capability

- Juniper NetScreen Firewalls models NS5gt, N25, NS50, NS500, NS204, NS208, NS5200, NS5000, SSG5, SSG20, SSG140, ISG 1000, ISG 2000. Some reverse engineering may be required depending on firmware revisions.
- Juniper Routers: M320 is currently being worked on and we would expect to have full support by the end of the 2010.

Recommendations and Expected Outcomes

- Discover Juniper equipment on networks in hard target countries to assess potential Juniper exploitation opportunities with existing capabilities.
- Assess potential additional targetable networks if additional equipment models could be exploited (e.g. if we could exploit MX-series routers, then networks X, Y, & Z could be exploited).
- Assess an effort to exploit the JUNOS operating system.

ORIGINATOR [redacted] NSA Integree to GCHQ Access Strategy Team (OPA-ACD), [redacted] 03FEB11

Table of Contents

Executive Summary **1**

Juniper Overview **2**

Juniper Corporate History 2

Current product series 3

Juniper as a Target **4**

Juniper as a Threat **5**

Target Usage of Juniper **5**

Current and Planned Work to Exploit Juniper **5**

Assessment of Potential Opportunity **6**

Recommendations and Expected Outcomes **6**

Juniper Overview

Juniper Corporate History

Juniper Networks, Inc. (NYSE:JNPR) headquartered in Sunnyvale, California, USA is a high-performance Internet Protocol network products company founded in 1996. Juniper's main products include *T-series*, *M-series*, *E-series*, *MX-series*, and *J-series* families of routers, *EX-series* Ethernet switches, and NetScreen and SRX-series security products. Juniper's JUNOS network operating system runs on most Juniper products.

In 1995 Pradeep Sindhu, a principal scientist at Xerox's Palo Alto Research Center, returned from vacation with the idea to start a company to supply high-performance routers to support the quickly emerging Internet. Sindhu started the company in February 1996 with $200,000 in seed money. He recruited engineers Bjorn Liencres from Sun Microsystems and Dennis Ferguson from MCI. For business expertise Sindhu recruited Scott Kriens, co-founder of StrataCom. Juniper

considers technology development to be a strategic advantage and despite the economic downturn in 2008 famously decided against cuts in the $800M R&D budget.

Juniper shipped its first product, the *M40* router, in September 1998. The product was a first-ever implementation of packet forwarding that could sustain line-rate packet forwarding across eight OC48c ports in a half-rack form factor. This was a critical technological improvement that allowed unconstrained Internet growth and gained Juniper a place in a market formerly dominated by Cisco Systems. Juniper maintained market momentum by delivering the M160 achieve OC-192 forwarding rates. By 2000 Juniper took 30% of the Internet core router market.

In 2002 Juniper announced the T640 capable of 40 Gigabit/slot performance and terabit-level system scaling. In 2002 Juniper also announced plans to expand its line of Internet core routers to the edge and started scoping other markets such as enterprise routing/switching and security. By the end of 2002 Juniper had penetrated the broadband aggregation segment with the Juniper E-series. This move towards the edge was further supported by extending the Juniper M-series technology towards network edge with M40e (2002)and M7i-M10i (2003) systems. Next, Juniper moved into enterprise and security space with technology acquired from NetScreen Technologies as well as the internally developed low-end J-series router family.

In 2006 Juniper delivered a highly-integrated, edge-specific 10 Gbit/s chipset (I-Chip) that formed the basis for a highly redundant M120 edge router and the Juniper MX-series of Ethernet-specific carrier routers. Driven by the growing importance of Ethernet services MX-series gained in excess of 250 accounts in less than 18 months and lends its hardware to SRX-series security appliances. The 2009 generation of MX delivers up to 120Gbps (full-duplex) per slot.

In 2007 on the core side of the business Juniper released a 100Gbps/slot Juniper T1600 router. The T1600 was the densest core router commercially available going into 2010 and is the first product to deliver a commercial implementation of the 100GE interface (802.3ba).

JUNOS is the in-house Operating System that runs on most of Juniper's networking equipment spanning routing, switching and security platforms. JUNOS was the first commercially available full-fledged modular OS with full memory protection available for routing products. JUNOS competes against other modular systems such as Cisco IOS-XR and Alcatel-Lucent SR-OS. JUNOS features both vertical and horizontal modularity, and provides APIs for third-party applications known as "JUNOS Space". Although JUNOS was originally derived from FreeBSD subsequent product development resulted in major kernel and infrastructure improvements like In-Service Software Upgrade and real-time packet forwarding plane.

Current product series

- *E-series* routers are broadband edge routers. The E series was developed by Unisphere, which Juniper acquired in 2002. The E series routers run the JUNOS operating system inherited from acquisition of Unisphere. The J, M, T, and MX series routers run JUNOS.
- *J-Series* routers are small customer-premises equipment or enterprise routers.
- *M-series* routers are multiservice edge routers.
- *T-series* routers are large core routers.
- *MX-series* routers are Ethernet services routers.

EX Series Switches - Juniper's switch products were introduced in 2008 and run JUNOS. Available in fixed and modular form factors with full or partial PoE functionality, EX represents Juniper's bid

for enterprise and cost-optimized Ethernet markets, augmenting the "One Operating System" strategy and generating $74 million in revenue during 4Q2009.

SRX Series Dynamic Service Gateways is a series of security services devices running JUNOS. Ranging from branch-office models to the SRX 5800, the world's fastest firewall. Combines security, routing and switching in one chassis. Security features include the full UTM functionality previously found on ScreenOS, including web filtering, IDP and anti-virus.

The *NetScreen SSG Series* and *ISG Series* firewalls run the ScreenOS operating system and provide firewall, anti-virus, intrusion protection and VPN services. Acquired with NetScreen Technologies, they run ScreenOS rather than JUNOS. These target small and medium−sized business. The ISG series is capable of more advanced IDP and virtualisation functionality and higher performance.

Secure Access products provide SSL-based VPN services to remote users without specialized clients. *NSM* Network and Security Manager is an enterprise-wide management tool for Juniper devices that features single-point bastion control over multiple Juniper devices, a syslog host and configuration backup repository, and the NSMXpress appliance that provides distributed hierarchical features.

Intrusion detection and prevention appliances.

Other Products

- *WX* and *WXC* ─ *series* WAN Accelerators -
- *UAC* Unified Access Control
- *Odyssey Access Client* - 802.1x supplicant
- *Security Threat Response Manager (STRM)*- Juniper sells an OEM version of Q1 Labs' QRadar product running on Juniper hardware.

Juniper's principal subsidiaries hold its international operations. They include Juniper Networks K.K. (Japan), Juniper Networks B.V. (Netherlands), Juniper Networks International Limited (Cayman Islands), Juniper Networks FSC Inc. (Barbados), Juniper Networks U.K. Ltd. (United Kingdom), Juniper Networks GmbH (Germany), Juniper Networks France Sarl (France), Juniper Networks Australia Ltd. (Australia), Juniper Networks Hong Kong Ltd. (Hong Kong), Juniper Networks South Asia Ltd. (Hong Kong), Juniper Networks China Ltd. (Hong Kong), Juniper Networks Canada Inc. (Canada), Juniper Networks International, Inc and Juniper Networks India Pvt Ltd (India).

Juniper as a Target

While Juniper is not necessarily the market share leader in any one space, they are a strong competitor and technology leader across several important markets from a SIGINT perspective. Juniper is at the core of the Internet in many countries by virtue of providing the highest density routers for many years. As telecommunications service providers move toward all IP networks, Juniper will play an increasingly central role in converged networks. Juniper has proven adept at leveraging their high density server technology to challenge market leaders in both the edge server and enterprise network firewall markets. In another somewhat niche market but one that is very important to SIGINT, Juniper is viewed as the ablest competitor selling SSL VPN technology.

- Well Established Position in the Carrier Space with high density routers
- Credible competitive alternative to Cisco dominance of core routing

- Carrier Ethernet Growing in Volume and Scope
- IP Traffic Growth Continues Unabated

Juniper as a Threat

Juniper's leadership in core IP routing and the Enterprise Network Firewall and SSL VPN markets means that the SIGINT community should keep up with Juniper technology to be positioned to maintain CNE access over time. The threat comes from Juniper's investment and emphasis on being a security leader. If the SIGINT community falls behind, it might take years to regain a Juniper firewall or router access capability if Juniper continues to rapidly increase their security.

Target Usage of Juniper

Global IP Networks – Juniper core routers can be found throughout the Internet and all other high capacity IP networks. Examples are too numerous to cite. A FLAG Telecom case study is available as an example.

Pakistan – Juniper firewalls are central to the very high priority HEADRESS NU project targeting a Pakistan government/military secure network. While the core Internet routers in Pakistan are all Cisco, Juniper is often seen as an edge router on networks connected to the core. Juniper routers are deployed in the Mobilink network and possibly Telenor.

Afghan - No evidence of Juniper presence

CT Broker - Although Juniper has been mentioned in connection with the Broker target on a number of occasions, the only evidence that has been seen is of a Juniper router being used in a small scale trial that wasn't taken any further.

CT Yemen - Juniper provide Security Hardware for the Yemen Telecom and a firewall for TeleYemen's VoIP connection to Verizon.

CT Saudi Arabia -

China – Juniper have a strong presence in China through Juniper Networks China Ltd. Based in Hong Kong. A Jiangxi eGovernment case study is available as an example. A press release is included below as another example of Juniper in China.

Juniper Networks Routing Platforms Form Core of China's Next-Generation Internet

T-series Core Platform and M-Series Multiservice Routers Provide Infrastructure for World's Largest IPv6 Network

SUNNYVALE, Calif., November 30th, 2005 - Juniper Networks, Inc. (NASDAQ: JNPR) today announced that its M- and T-series routing platforms have been selected for the core of the China Next Generation Internet (CNGI) project. The CNGI project is a Chinese government-funded initiative to promote Internet Protocol version 6 (IPv6) throughout China, and is expected to become the largest IPv6 network in the world. Juniper Networks platforms were selected for their proven, industry-leading IPv6 capabilities, and will be deployed in CNGI's participating networks, including the China Education and Research Network (CERNET2), China Mobile, China Netcom, China Railcom, China Telecom and China Unicom.

Current and Planned Work to Exploit Juniper

GCHQ currently has exploit capability against:

- Juniper NetScreen Firewalls models NS5gt, N25, NS50, NS500, NS204, NS208, NS5200, NS5000, SSG5, SSG20, SSG140, ISG 1000, ISG 2000. Some reverse engineering may be required depending on firmware revisions.
- Juniper Routers: M320 is currently being worked on and we would expect to have full support by the end of the 2010.
- No other models are currently supported.
- Juniper technology sharing with NSA improved dramatically during CY2010 to exploit several target networks where GCHQ had access primacy.

Assessment of Potential Opportunity

The ability to exploit Juniper servers and firewalls will pay many dividends over the years. Juniper is already a major hardware provider across the Internet today. With the growth of converged IP networks and Juniper's technology leadership we should expect Juniper opportunities to grow significantly over the next several years. Juniper is a strong competitor to Cisco when a buyer seeks an alternative supplier who is also a technology leader. Huawei is another competitor in the same space when a buyer seeks a lower cost alternative supplier.

Juniper carries a potential opportunity and complication by being a US company. There is potential to leverage a corporate relationship should one exist with NSA. Any GCHQ efforts to exploit Juniper must begin with close coordination with NSA.

The Juniper family of products are somewhat homogenous in their use of the JUNOS operating system. This could create opportunities to exploit security vulnerabilities in JUNOS and extrapolate them to a wider range of Juniper routing product lines.

Recommendations and Expected Outcomes

2. Exploit What's Available Today (EWAT): *Capture Existing Opportunities*

- Document current capabilities to exploit Juniper equipment.
- Discover Juniper equipment on networks in hard target countries (potential Juniper exploitation opportunities).
- Validate potential Juniper exploitation opportunities against 1) fit with current Juniper exploit capabilities 2) target centric evaluation of potential intelligence benefit.
- Impact assessments against validated Juniper exploitation opportunities and business decision to pursue or not.

3. Expand Juniper Exploit Capabilities: *Create Future Opportunities*

- Discover Juniper equipment on networks in hard target countries (potential Juniper exploitation opportunities).
- Assess potential additional targetable networks if additional equipment models could be exploited (e.g. if we could exploit MX-series routers, then networks X, Y, & Z could be exploited).
- Assess potential intelligence benefit if additional networks could be exploited.
- Impact assessments of creating exploits of additional Juniper models.

4. JUNOS Exploitation:

- The vast majority of current Juniper exploits are against firewalls running the ScreenOS operating system.
- Juniper will migrate all products to the JUNOS operating system over time.
- An effort to ensure exploitation capability of JUNOS should bear fruit against a wide range of Juniper products.