July 17, 2020

The Honorable Ron Wyden

United States Senate

221 Dirksen Senate Office Building

Washington, DC 20510

Senator Wyden:

I am writing in response to the June 10, 2020 inquiry from you and your Congressional colleagues to Juniper Networks ("Juniper") requesting an update to our 2015 public disclosure of the remediation of unauthorized code in Juniper's legacy ScreenOS operating system.

There has been considerable public debate recently regarding industry-wide cybersecurity practices and policy. We welcome this opportunity to be a part of both the dialogue and the solution. More specifically, we understand that these policy debates have generated concerns that technology companies could intentionally include so-called "backdoors" in products. To be clear - Juniper does not and will not deploy backdoors, and we are opposed to any legislation mandating backdoors.

Juniper Networks

Juniper is a United States-headquartered, publicly traded company that produces internet networking solutions. Founded more than two decades ago, Juniper provides innovative and secure networks to service operators and enterprises. Headquartered in Sunnyvale, California, we currently have more than 9,000 employees in more than 100 offices around the world; including Westford, Massachusetts; Bridgewater, New Jersey; and Herndon, Virginia.

In our business, security is a critical factor at every point in the network. Juniper makes some of the most innovative and sophisticated routers, switches, security products and networking software in the world. We supply these products to multiple security-sensitive industries and agencies, including highly-regulated financial services and healthcare organizations; the world's biggest and busiest wired and wireless carriers; content and internet service providers; cloud and data center providers; cable and satellite operators; as well as, security-conscious federal agencies. Our responsibility to our customers is our highest priority and we have consistently evangelized the need for threat-aware networks and a comprehensive, robust approach to network security.

Juniper has a long history of providing networking and security services to federal agencies and partners. Since Juniper's inception, we have provided networking services to the federal government, which we proudly continue today as a mission critical partner to all components of the Department of Defense, the Intelligence Community and civilian departments and agencies. We work hand-in-hand with our federal customers on network modernization, automation and security to fulfill essential requirements.

1133 Innovation Way p +1 408 745 2000
Sunnyvale, CA 94089 f +1 408 745 2100

Juniper and 5G

We are part of a small group of U.S. companies in our industry that plays a critical role in 5G infrastructure buildouts. Service providers will need to accommodate an exponential growth in internet traffic, operational complexities, emerging security threats and high-performance demands; Juniper's 5G offerings will be pivotal in powering this transformation. Our software solutions give service providers the ability to transform their networks into secure, automated and cloud-ready infrastructures. Our engineers have spent years engaging with international standards bodies to prevent others from locking in technology that might not serve cybersecurity interests. Our patents similarly protect the role of U.S. technology in communications and computing.

As you might be aware, we also face rigorous competition in 5G from within the U.S. and Chinese companies, including Huawei and ZTE. This competition puts Juniper on the front line to ensure the leadership of the United States and its allies and to secure future communications and computing.

The 2015 Disclosure and Dual_EC DRBG

As we disclosed in 2015, Juniper suffered intrusions believed to have been carried out by a sophisticated nation-state hacking unit. Juniper became aware that an attacker had gained access to a proprietary Juniper network which gave the attacker an ability to review and change the source code for ScreenOS. The attacker was able to do this in a way that bypassed security measures that protected the integrity of the code. The attacker used intrusion techniques characteristic of advanced and persistent threat actors to carry out their attacks; the intrusion was neither caused nor aided by the use of Dual_EC_DRBG.

Once Juniper identified the unauthorized code, we immediately engineered a remediation for all impacted versions of ScreenOS and publicly announced the issue. In doing so, we urged our customers to either deploy the patched ScreenOS or transition to our then-current operating system, Junos OS, which was not impacted by this event. This was and is consistent with the practice of other software companies, all of whom regularly patch new vulnerabilities and alert customers to the need for an update.

Our 2015 disclosure candidly stated the severity of the security risks the intrusion created and the urgency of remediation, but it did not provide details that might compromise Juniper proprietary information. Given the competitive environment we face, that is a policy we are continuing to observe.

Juniper investigated the scope and source of the intrusion in several ways. We retained an outside incident response and forensics firm to assist us in investigating the intrusion and provide us with details about the tactics and tools used to carry out the attack. We also reported the attack to the Federal Bureau of Investigation, cooperated with them and exchanged relevant information about the attack.

The specific unauthorized code and the resultant vulnerabilities have been the subject and content of previous Juniper advisories. We believe we successfully remediated the attack and, more importantly, enhanced the security of our network and code. To this day, customers that manage sensitive networks, from governments to cloud and service providers, continue to rely on us for secure networking solutions.

1133 Innovation Way p +1 408 745 2000
Sunnyvale, CA 94089 f +1 408 745 2100

Juniper relies heavily on NIST and its standards in designing products. This was also our practice with respect to Dual_EC_DRBG, an encryption algorithm standardized in NIST SP800-90A that other major U.S. technology companies also deployed. We recognize that the algorithm has since been withdrawn by NIST due to security concerns and, in 2016, we publicly announced the removal of the implementation of the withdrawn algorithm from ScreenOS, an operating system that was already in the process of being retired from Juniper's security product set. Junos OS, the operating system in place since 1998, relies on NIST standards but has *never* used the Dual_EC_DRBG algorithm.

Juniper's Policy on Backdoors

As noted above, we understand that there is a vigorous policy debate about whether and how to provide government access to encrypted content. Juniper certainly shares concerns about policies that would degrade user security of our products. We can assure you that, as a matter of policy, Juniper does not and will not insert backdoors into its products and we oppose any legislation mandating backdoors.

Juniper appreciates the opportunity to clarify the matters raised in your letter and your longstanding interest in internet security. We hope to continue to work with you on sound public policy in this critical area.

Sincerely,

Brian Martin

Senior Vice President,

General Counsel and Secretary

Juniper Networks, Inc.

1133 Innovation Way p +1 408 745 2000
Sunnyvale, CA 94089 f +1 408 745 2100