

Congress of the United States

Washington, DC 20515

June 10, 2020

Rami Rahim
Chief Executive Officer
Juniper Networks
1133 Innovation Way
Sunnyvale, CA 94089

Dear Mr. Rahim,

We write to seek information about Juniper Networks' investigation of several likely backdoors in its NetScreen line of firewalls.

In December of 2015, Juniper announced that it had discovered unauthorized code in the software it distributed to customers between 2012 and 2015 for its NetScreen firewalls. Soon after Juniper revealed this security breach, cybersecurity researchers determined that the code was likely an encryption backdoor that could be exploited by a sophisticated adversary to unmask the encryption used to protect data flowing over virtual private networks.

Alarming, the suspicious code that Juniper discovered in 2015 did not create the backdoor — it apparently modified one that was seemingly already there. Subsequent analysis by an international team of leading experts determined that, in fact, a backdoor had likely been added to Juniper's products as far back as 2008. According to the researchers, the unauthorized code Juniper discovered in 2015 merely changed the keys to this pre-existing backdoor.

The researchers determined that sometime between 2008 and 2009, Juniper quietly added a National Security Agency (NSA) designed encryption algorithm to its products. This encryption algorithm, known as Dual_EC_DRBG, had, since 2005, been the subject of criticism by independent cryptographers who argued that it probably contained a backdoor. In spite of these warnings, the National Institute of Standards and Technology (NIST), which issues U.S. government standards for encryption algorithms, standardized Dual_EC_DRBG in 2006. However, after Edward Snowden's disclosures in 2013, NIST withdrew the algorithm. In a post-mortem published in 2014, a senior NIST cryptographer confirmed that NSA had in fact created Dual_EC_DRBG, that he had been told that NSA did not want to answer questions about possible backdoors, and that, in retrospect, it "should not have been included" in the official NIST standard.

Soon after Juniper revealed in 2015 that it discovered unauthorized code in its products, Juniper announced that it was conducting an investigation into the matter. According to media reports at the time, the Federal Bureau of Investigation also launched an investigation. It has now been over four years since Juniper announced it was conducting an investigation, but your company has still not revealed what, if anything, it uncovered. The American people — and the companies and U.S. government agencies that trusted Juniper's products with their sensitive data — still

have no information about why Juniper quietly added an NSA-designed, likely-backdoored encryption algorithm, or how, years later, the keys to that probable backdoor were changed by an unknown entity, likely to the detriment of U.S. national security.

Over the past year, Attorney General William Barr and other senior government officials have renewed their call for technology companies to subvert the encryption in their products in order to facilitate government surveillance. Juniper's experiences can provide a valuable case study about the dangers of backdoors, as well as the apparent ease with which government backdoors can be covertly subverted by a sophisticated actor. To that end, we would appreciate answers to the following questions by July 10, 2020:

1. In August of 2009, Juniper obtained joint certification from the U.S. and Canadian governments, certifying that Juniper's Netscreen products running ScreenOS satisfied the Federal Information Processing Standards (FIPS) for cryptographic modules. Despite the fact that Dual_EC_DRBG was then a FIPS-certified algorithm, Juniper did not disclose the inclusion of Dual_EC_DRBG in its FIPS application, although Juniper disclosed the use of several other FIPS-certified algorithms. Why did Juniper not disclose to NIST that its products used the Dual_EC_DRBG algorithm?
2. Rather than using the "Q" value for the Dual_EC_DRBG algorithm specified in the NIST standard, Juniper used a different Q value when it originally added Dual_EC_DRBG to its products, sometime between 2008-2009. Please explain why Juniper opted to use a different Q value, how it was generated and by whom. If Juniper did not generate this Q value following the procedures described in NIST Special Publication 800-90, please explain why.
3. What were the results of Juniper's investigation following its 2015 discovery of unauthorized code?
 - a. Who was responsible for conducting the investigation?
 - b. What was the scope of the investigation?
 - c. If a written report was produced, please provide us with a copy.
4. Did the investigation examine Juniper's decision to add and retain support for the Dual_EC_DRBG algorithm in Juniper's ScreenOS software, long after cryptography experts publicly raised serious questions regarding a potential backdoor in Dual_EC_DRBG? If not, why not?
5. According to the research team that studied the Juniper backdoors, at or around the same time that Juniper added support in ScreenOS for the Dual_EC_DRBG algorithm, Juniper also increased the Internet Key Exchange nonce size from 20 bytes to 32 bytes. The research team argues that this change would make it easier for a sophisticated adversary to exploit backdoors in Dual_EC_DRBG. Did Juniper's investigation look into the decision to increase the size of the nonce? If yes, what did Juniper discover? If not, why not?
6. Please identify the Juniper employees who approved the changes to ScreenOS described in questions 4 and 5.
7. Did Juniper's investigation uncover any information relating to the source of the unauthorized code revealed by Juniper in December 2015, and in particular, the code that altered the Q value in the Dual_EC_DRBG algorithm?

8. Did the results of the investigation include any recommendations to prevent future security incidents? If yes, has Juniper implemented all of the recommendations?

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in Senator Wyden's office.

Sincerely,



Ron Wyden
United States Senator



Michael S. Lee
United States Senator



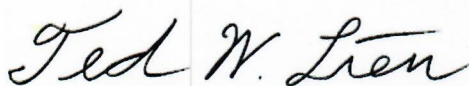
Cory A. Booker
United States Senator



Jerrold Nadler
Chairman
Committee on the Judiciary



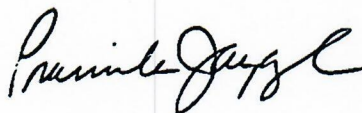
Bennie G. Thompson
Chairman
Committee on Homeland Security



Ted W. Lieu
Member of Congress



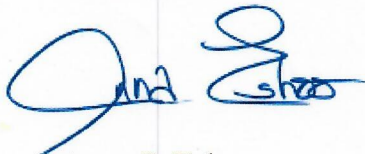
Zoe Lofgren
Member of Congress



Pramila Jayapal
Member of Congress



Tom Malinowski
Member of Congress



Anna G. Eshoo
Member of Congress



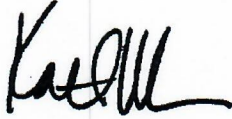
Bill Foster
Member of Congress



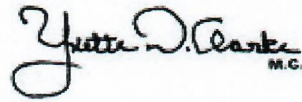
Ro Khanna
Member of Congress



Suzan K. DelBene
Member of Congress



Kathleen M. Rice
Member of Congress



Yvette D. Clarke
Member of Congress



Cedric L. Richmond
Member of Congress