Finite State report fails to tell the whole story

Huawei is serious about cyber security and welcomes any objective input that makes our technology more secure. This includes analyses that publicly disclose any weaknesses our products may have.

On June 25, a US cyber security firm called Finite State released a report saying Huawei products were more vulnerable than equipment made by some of our competitors. We have a Product Security Incident Response Team (PSIRT) that discloses vulnerabilities in our products when we find them. PSIRT and our engineers published an in-depth response to the technical points of Finite State's analysis.

The Finite State report is a preliminary assessment, very much like the ones Huawei (and every vendor of network equipment) conducts to test the integrity of our products. As a preliminary assessment, it does not tell the whole story.

Our initial review suggests that the data cited in their report, and the testing methods they used, would not identify significant vulnerabilities in Huawei's gear.

First, many of the products critiqued are for enterprise markets, with some data center switches for the carrier market. None of the Huawei products tested by Finite State will be deployed for 5G RAN or Core in telecommunications networks. (Products made by Cisco, the largest provider of gear for the enterprise market, were not tested.)

Second, Finite State used something called a binary image analysis tool. The tool is suitable for certain narrow security applications but cannot provide a complete and accurate picture of security vulnerabilities in the products tested.

Third, Finite State specializes in security for the Internet of Things (IoT) and may not fully understand how telecommunications equipment is deployed. For example, an important fact not referenced in the report is that after installation, default settings are zeroed out, providing network operators with secure control over their equipment. Equipment vendors also work closely with operators to address potential vulnerabilities, such as those that might be disclosed using a tool like the one Finite State used for this study.

Fourth, Finite State tested older versions of Huawei software, which might not have contained important security patches issued later. It is not clear why Finite State chose older versions when newer ones were available. We don't know how Finite State obtained the software they used, and we don't know which distribution channel they used as a source.

Finally, and significantly, Finite State did not give Huawei a chance to review its analysis before publication. Normally, firms that conduct independent analysis strive to present neutral, unbiased research; accordingly, they check any findings with the affected vendors before going public. Finite State's failure to do that raises questions about their motivation in releasing the report. More importantly, the report lacks important insights that could have been provided to make it more complete, and more accurate.

The inclusion of extraneous, negative information about Huawei also suggests that objectivity was not a major consideration. For example, several pages outline "Key security concerns" about Huawei, setting a negative tone at the outset and suggesting a presumption that Huawei products are flawed.

Finite State also cited a Bloomberg story which incorrectly reported that Vodafone had found "backdoors" in Huawei's network gear in Italy. Vodafone quickly corrected the report, explaining that what Bloomberg had mistakenly called a backdoor was, in fact, part of a routine diagnostic function commonly used in the telecommunications industry. Yet, although Vodafone published the official statement in April, Finite State's June report still cited the erroneous Bloomberg story and did not mention the correction.

Huawei is committed to securing critical network infrastructure. We work with independent researchers and testing firms worldwide to find, and fix, vulnerabilities that might compromise security. Because we are headquarted in China, we are probably the most frequently, most thoroughly tested technology provider in the world. Even so, no one has ever found any evidence of cyber security wrongdoing in our equipment. Because of the important insights gained from expert, independent reviews of our technology, we will spend US$2 billion in the coming years to revamp our software engineering processes and improve our software quality and security.

Again, we have no problem letting people pick apart our software; in fact, we have facilities dedicated to doing just that. But the testing methodology employed by Finite State is not, by itself, sufficient to provide what the global community needs: an objective, transparent method of testing the products sold by technology providers based on uniform global standards.

That said, we would welcome the opportunity to speak with Finite State about their findings, in hopes of gaining insights that can help us improve our practices and further inform our software engineering revamp.

Finite State's report implicitly supports Huawei's longstanding call for independent, third-party testing of products from all equipment vendors, using internationally recognized standards. Such an approach would help move important conversations about cyber security away from the realm of politics, toward the domain of science, engineering, and facts. And that would help make cyberspace a safer place.

July 9, 2019
Huawei Technologies Co., Ltd.