UK cyber security officials report Huawei’s security practices are a mess

Enlarge / As Huawei makes its bid to roll out 5G, a UK government oversight board is not exactly thrilled with the company’s security practices—or how it makes software.
Getty Images

reader comments

9 with 9 posters participating

Share this story

In November of 2010, the Chinese networking and telecommunications giant Huawei entered into an agreement with the government of the United Kingdom to allow extensive security reviews of Huawei’s hardware and software—a move intended to belay fears that the company posed a security risk to the UK’s networks. Since then, the Huawei Cyber Security Evaluation Centre (HCSEC) has given UK officials a window into the company’s information security practices. And UK officials haven’t necessarily liked what they’ve seen.

In a report issued today, the HCSEC Oversight Board—a panel including officials from the National Cyber Security Centre, GCHQ and other agencies, as well as a senior executive from Huawei—warned that Huawei had failed to make long-promised changes to its software development and engineering practices needed to improve security.

“HSCE’s work has continued to identify concerning issues in Huawei’s approach to software development bringing

significantly increased risk to UK operators," the oversight board members noted. "No material progress" had been made in correcting those problems since they were noted last year.

In addition, audits and reviews by the HSCE had found "further significant technical issues in Huawei's engineering practices," the board noted. And while Huawei had promised to make major investments in correcting its problems—promising to invest $2 billion in security engineering improvements over five years—the board remained unconvinced based on their review:

At present, the Oversight Board has not yet seen anything to give it confidence in Huawei's capacity to successfully complete the elements of its transformation programme that it has proposed as a means of addressing these underlying defects. The Board will require sustained evidence of better software engineering and cyber security quality verified by HCSEC and NCSC. Overall, the Oversight Board can only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term.

This report comes as Huawei is posed to play a major role in the deployment of 5G wireless communications in the UK, despite the US government's insistence that Huawei gear poses a security threat. The Trump administration contends that because of Huawei's connections to the Chinese government and military, the company's software and hardware could be used by China's Ministry of State Security or the Peoples' Liberation Army for espionage or sabotage.

The problems unearthed by HCSEC, however, suggest that the bigger threat is that Huawei gear could be hacked by just about anyone who cared to make an effort. And because of how Huawei runs its software development, it's impossible to give blanket certification of any one product's security.

One major problem cited by the report is that a large portion of Huawei's network gear still relies on a version of Wind River's VxWorks real-time operating system (RTOS) that has reached its "end of life" and will soon no longer be supported. Huawei has bought a premium long-term support license from VxWorks, but that support runs out in 2020. That could leave hardware installed by telecommunications carriers at risk.

And while Huawei is developing its own RTOS to eventually replace VxWorks, there's reason for concern about how secure that OS will be—because Huawei's software development process is not exactly reliable. HCSEC reported that the software build process used by Huawei results in inconsistencies between software images. In other words, products ship with software with widely varying fingerprints, so it's impossible to determine whether the code is the same based on checksums.

Despite efforts by the UK to get Huawei to improve its configuration management processes dating back to 2010, the company has applied configuration management inconsistently from product to product. For example, during an on-site visit to Huawei's Shanghai development center by the board, it was discovered that "an unmanageable number" of versions of the OpenSSL library were allowed to be used in products—including some with known vulnerabilities. "The conclusion reported back to the Oversight Board is that Huawei's basic engineering process does not correctly manage either component usage or the lifecycle sustainment issues, leaving products unsupportable in general," the report states.

As a result, the board noted, "it is hard to be confident that different deployments of similar Huawei equipment are broadly equivalently secure." The lack of consistent software builds means it's difficult (at best) to determine whether a bug found in one version of software has been fully patched in another build.

There are some other challenges regarding the RTOS. Huawei's in-house RTOS is based on the Linux kernel, and it's not clear how well it will integrate with existing Huawei code. Officials from the National Cyber Security Centre performed a review of the RTOS development effort at Huawei's facility in Shanghai and concluded that they "did not have sufficient evidence to be confident in the long-term sustained engineering of Huawei'sown real time operating system," the board members noted. Combined with the challenges of integrating old software written for the VxWorks RTOS (which has a single user, single memory space architecture) over to a Linux-based OS, this all poses significant long-term risks for network operators, the board found.

https://arstechnica.com/?p=1482557