UK Government Issues Report on Huawei Vulnerabilities

Skadden

04 / 16 / 19

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

Four Times Square
New York, NY 10036
212.735.3000

Introduction

On March 28, 2019, the Oversight Board of the United Kingdom's Huawei Cyber Security Evaluation Centre (HCSEC)[1] released a report identifying "serious and systematic defects in Huawei's software engineering and cyber security competence." This report — the fifth annual review of Huawei products used in British telecommunications networks — represents the most detailed public expression of concern regarding security vulnerabilities in Huawei products by a national government to date, and bolsters, with significant technical detail, the concerns that U.S. government officials have raised about Huawei. Although the report states that the issues are not believed to be the result of Chinese state interference, the issues identified in the report are nonetheless serious enough that the Oversight Board found that it could offer only "limited assurance" that long-term security risks can be managed in the Huawei equipment currently employed in U.K. networks. The report is important not only for providing insight into how the U.S. and other allied governments may perceive Huawei and, thus, companies that use Huawei equipment, but for providing technology companies guidance on where to focus their own security and product integrity efforts.

Summary of the HCSEC Oversight Board's Findings

In evaluating more than three dozen products, the HCSEC identified "significant, concerning issues in Huawei's approach to software development bringing significantly increased risk to U.K. operators," including major defects in general software engineering and cybersecurity quality. The evaluation uncovered, among other things, the following issues:

- Huawei's build process continues to provide no end-to-end integrity or adequate configuration management. Without this baseline of integrity, the HCSEC cannot routinely confirm that the products they are testing are the same as the products used in U.K. networks, or perform true root cause analysis of any issues identified in the products. Particular build process issues identified in the report included the use of unclean virtual machines in the build process, poor management of the build environment resulting in unnecessary or duplicate tools being installed, and poor management of source code across development teams and poor integration of components in the products.
- Huawei uses an old, and soon-to-be out of mainstream, support version of a third-party real-time operating system that is subject to increased risk as a result of its out-of-date design. Huawei also did not provide a credible plan to reduce the risk of its use of this operating system or a path to upgrade to a supportable operating system that is appropriate for carrier-grade telecommunications systems.
- Huawei's software component lifecycle management revealed significant flaws that could lead to cybersecurity and availability risk. For example, the HCSEC found evidence of extensive non-adherence to basic secure coding practices, the incorrect use of safe memory manipulation functions, and the inappropriate suppression of warnings from static analysis tools.

Perhaps most troubling, the annual report noted that Huawei made no material progress on the software engineering and cybersecurity issues that the Oversight Board identified in its 2018 report, nor has the company made any credible plans to mitigate or remediate

[1] The HCSEC is a Huawei facility that opened in November 2010 to provide the British government with insight into Huawei products and operations and help mitigate any perceived risks arising from the use of Huawei products in U.K. critical national infrastructure.

UK Government Issues Report on Huawei Vulnerabilities

the risks posed by its products. Although Huawei announced its intention to transform its software engineering processes through a $2 billion investment over the next five years, it has not supported this claim with any material and verifiable actions.

Key Takeaways

The HCSEC Oversight Board's report may complicate the vendor selection process for companies considering using Huawei equipment on their networks in the U.K., the United States and, likely, their close allies. Indeed, although the report stated that the HCSEC Oversight Board did not believe Huawei's problems were the result of Chinese state interference, in a way, this conclusion may be more damaging to Huawei because it serves as a counterpoint to Huawei's claims that the critiques levied against it are merely warrantless geopolitical attacks. Rather than vague national security concerns, the report documents in great detail the security problems with Huawei equipment. Companies using Huawei equipment and seeking legal or regulatory approvals in the United States, such as through the Committee on Foreign Investment in the United States (CFIUS) or the Federal Communications Commission's Team Telecom process, can expect this report to only further solidify those entities' concerns about Huawei.

In addition, apart from the use of Huawei equipment specifically, companies can expect the issues highlighted by the HCSEC Oversight Board to be raised with other equipment makers in the context of government reviews and licensing scenarios globally, including in the transactional and export licensing spaces. For instance, foreign companies seeking to acquire U.S.-based technology companies may expect CFIUS to scrutinize cybersecurity, product development and supply chain concerns during the review process. These issues also could be examined in the foreign direct investment review processes in other countries and regions, such as in the European Union. Moreover, software engineering and cybersecurity practices could arise in the export control licensing context to ensure that products are consistent and secure.

Accordingly, hardware and software developers should compare the Oversight Board's findings against their own practices and, to the extent that companies have deficiencies similar to those identified by the Oversight Board, they should be treated as high-priority items. For example, developers should be mindful in ensuring that they are using secure coding practices and supportable components. It is also important for developers to consider controls and tools necessary to ensure build consistency across products and programs, manage components appropriately, and test for potential vulnerabilities. Finally, developers should consider the plans and mechanisms in place to obtain feedback on vulnerabilities, mitigate such vulnerabilities, and communicate the patches in an effective and efficient manner.

Contacts

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Donald L. Vieira
Partner / Washington, D.C.
202.371.7124
donald.vieira@skadden.com

Jennifer Ho
Associate / Washington, D.C.
202.371.7266
jennifer.ho@skadden.com

Nathan Mitchell
Associate / Washington, D.C.
202.371.7193
nathan.mitchell@skadden.com

Joe Molosky
Associate / Chicago
312.407.0512
joe.molosky@skadden.com