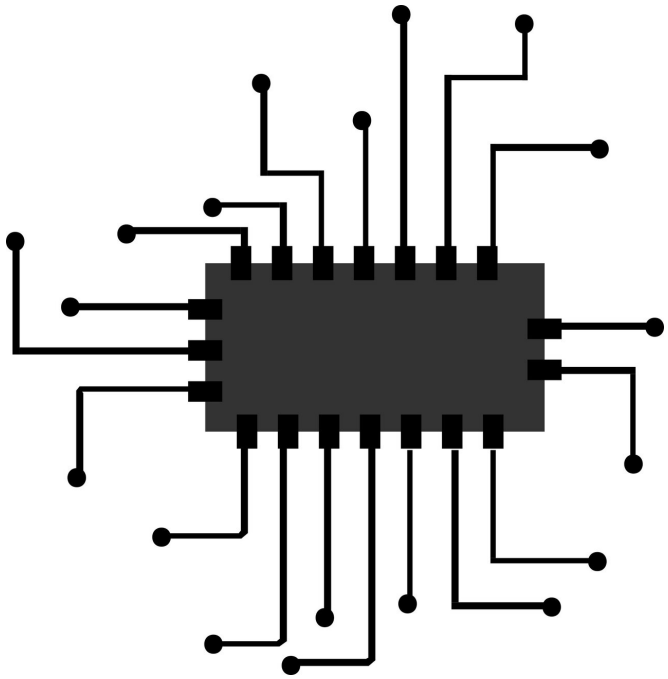
# Critical "Starbleed" vulnerability in FPGA chips identified

16 April 2020



Credit: CC0 Public Domain

Field programmable gate arrays, FPGAs for short, are flexibly programmable computer chips that are considered very secure components in many applications. In a joint research project, scientists from the Horst Görtz Institute for IT Security at Ruhr-Universität Bochum and from Max Planck Institute for Security and Privacy have now discovered that a critical vulnerability is hidden in these chips. They called the security bug "Starbleed." Attackers can gain complete control over the chips and their functionalities via the vulnerability. Since the bug is integrated into the hardware, the security risk can only be removed by replacing the chips. The manufacturer of the FPGAs has been informed by the researchers and has already reacted.

The security researchers will present the results of their work at the 29th Usenix Security Symposium to be held in August 2020 in Boston, Massachusetts, U.S.. The scientific paper has been available for download on the Usenix website since April 15, 2020.

**Focus on the bitstream**

FPGA chips can be found in many safety-critical applications today, from cloud data centers and mobile phone base stations to encrypted USB-sticks and industrial control systems. Their decisive advantage lies in their reprogrammability compared to conventional hardware chips with their fixed functionalities.

This reprogrammability is possible because the basic components of FPGAs and their interconnections can be freely programmed. In contrast, conventional computer chips are hard-wired and, therefore, dedicated to a single purpose. The linchpin of FPGAs is the bitstream, a file that is used to program the FPGA. In order to protect it adequately against attacks, the bitstream is secured by encryption methods. Dr. Amir Moradi and Maik Ender from Horst Görtz Institute, in cooperation with Professor Christof Paar from the Max Planck Institute in Bochum, Germany, succeeded in decrypting this protected bitstream, gaining access to the file content and modifying it.

**Market leader affected**

As part of their research, the scientists analysed FPGAs from Xilinx, one of the two market leaders in field-programmable gate arrays. The Starbleed vulnerability affects Xilinx's 7-series FPGAs with the four FPGA families Spartan, Artix, Kintex and Virtex as well as the previous version Virtex-6, which form a large part of Xilinx FPGAs used today. "We informed Xilinx about this vulnerability and subsequently worked closely together during the vulnerability disclosure process. Furthermore, it appears highly unlikely that this vulnerability will

occur in the manufacturer's latest series," reports Amir Moradi. Xilinx will also publish information on its website for affected customers.

**Advantage of the chips turns into disadvantage**

To overcome the encryption, the research team took advantage of the central property of the FPGAs: the possibility of reprogramming. This is done by an update and fallback feature in the FPGA itself, which revealed itself as a weakness and gateway. The scientists were able to manipulate the encrypted bitstream during the configuration process to redirect its decrypted content to the WBSTAR configuration register, which can be read out after a reset.

Thus, the advantage of individually reprogramming the chips turns into a disadvantage, as the scientists show in their research work—with severe consequences: "If an attacker gains access to the bitstream, he also gains complete control over the FPGA. Intellectual properties included in the bitstream can be stolen. It is also possible to insert hardware Trojans into the FPGA by manipulating the bitstream. Since the security gap is located in the hardware itself, it can only be closed by replacing the chip," explains Christof Paar, adding: "Although detailed knowledge is required, an attack can eventually be carried out remotely—the attacker does not even have to have physical access to the FPGA."

**More information:** Maik Ender, Amir Moradi, Christof Paar: The Unpatchable Silicon: A Full Break of the Bitstream Encryption of Xilinx 7-Series FPGAs, Usenix Security Symposium, Boston, MA, USA, 2020: www.usenix.org/conference/usen … 0/presentation/ender

Provided by Ruhr-Universitaet-Bochum