Una vulnerabilidad de hardware no reparable recientemente descubierta en los productos de lógica programable de Xilinx, permite a los hackers romper el cifrado de flujo de bits y clonar la propiedad intelectual, cambiar la funcionalidad o incluso, implantar troyanos de hardware.

Los detalles de los ataques contra Xilinx 7-Series y Virtex-6 Field Programmable Gate Arrays (FPGAs), se descubrieron en un documento titulado «*El silicio incompatible: una ruptura completa del cifrado de flujo de bits de Xilinx 7-Series FPGS*«, por un grupo de académicos del Instituto Horst Goertz para Seguridad Informática y el Instituto Max Planck para Seguridad Cibernética y Privacidad.

> *«Exploramos una falla de diseño que filtra por partes el flujo de bits descifrado. En el ataque, el FPGA se utiliza como un oráculo de descifrado, mientras que solo se necesita acceso a una interfaz de configuración. El ataque no requiere herramientas sofisticadas y, dependiendo del sistema de destino, puede ser lanzado de forma remota»*, dijeron los investigadores.

Estos hallazgos se presentarán en el Simposio de seguridad de USENIX a finales de este año. Los investigadores afirmaron que revelaron de forma privada los defectos a Xilinx el 24 de septiembre de 2019. El fabricante de semiconductores, en respuesta, publicó un aviso de diseño que reconoce la vulnerabilidad.

> *«La complejidad de este ataque es similar a los ataques DPA bien conocidos y probados contra estos dispositivos, por lo tanto, no debilitan su postura de seguridad»,* dijo la compañía.

Los FPGA son circuitos integrados programables que se pueden reconfigurar en el campo para que coincidan con una aplicación o funcionalidad deseada dependiendo de dónde se implemente. Debido a sus altos niveles de flexibilidad, los FPGA se utilizaron ampliamente en el desarrollo de redes móviles 5G, electrónica de consumo, centros de datos, tecnología

aeroespacial y automotriz.

Cabe señalar que Xilinx e Intel (a través de su adquisición de Altera), dominan el mercado de FPGA, con Xilinx solo representando casi el 50% de la cuota de mercado.

Debido a que los diseños de FPGA están codificados en flujos de bits, una vulnerabilidad de hardware de este tipo podría tener graves consecuencias, según los investigadores.

A diferencia de otros ataques de sondeo y canales laterales conocidos contra Xilinx y Altera FPGA, el novedoso ataque de *«bajo costo»* tiene como objetivo recuperar y manipular el flujo de bits al aprovechar la interfaz de configuración (como selectMAP o JTAG) para leer los datos del dispositivo FPGA.

Como característica, la *«relectura»* está destinada a ayudar a verificar que el diseño se descargó correctamente al dispositivo. Pero en un intento por proteger el diseño, el flujo de bits está encriptado (AES-256 en modo CBC) para evitar las lecturas en todos los puertos externos.

El ataque ideado por los investigadores se propone manipular el flujo de bits cifrado para redirigir sus datos de configuración descifrados a un registro de dirección de inicio de MultiBoot (WBSTAR o dirección de inicio de arranque en caliente), que permite cambiar entre imágenes sobre la marcha para actualizaciones y cargar un flujo de bits de reserva con un buen diseño conocido en el dispositivo FPGA.

Debido al uso de memoria flash para almacenar estos componentes, un reinicio no borra el contenido del registro. Como consecuencia, la confidencialidad del flujo de bits puede romperse de la siguiente forma:

- Crear un flujo de bits malicioso y un flujo de bits de lectura. El flujo de bits malicioso explota la maleabilidad del modo de cifrado CBC para alterar el comando en el flujo de bits, que escribe datos en el registro de configuración WBSTAR.
- Cargar el flujo de bits malicioso en el dispositivo FPGA.

- Un restablecimiento automático de la FPGA se produce debido a los cambios realizados en el flujo de bits en el paso 1, pero no restablece el contenido de WBSTAR, debido a que se utiliza para la función MultiBoot y fallback.
- Volver a leer el contenido de registro WBSTAR utilizando el flujo de bits de lectura.
- Restablecer manualmente el dispositivo FPGA para repetir los pasos anteriores y recuperar todo el flujo de bits cifrado como palabras de 32 bits.

> *«En resumen, el FPGA, si se carga con la clave de cifrado, descifra el flujo de bits cifrado y lo escibe para el atacante en el registro de configuración legible»,* dijeron los investigadores.
>
> *«Por lo tanto, el FPGA se utiliza como un oráculo de descifrado. El hecho de que solo se puedan descubrir palabras individuales de 32 bits en cada iteración determina la duración de descifrado del flujo de bits completo: en nuestros experimentos, podemos descubrir un complemento Kintex-7 XC7K160T bitstream en 3 horas y 42 minutos, por ejemplo».*

En el segundo tipo de ataque, el FPGA se puede utilizar para cifrar flujos de bits arbitrarios, una vez más aprovechando el modo CBC subyacente, y crear una etiqueta de autenticación de mensaje válida (HMAC), rompiendo así la autenticidad del flujo de bits también.

Según los investigadores, los ataques provienen de una trampa de que los datos del encabezado de flujo de bits se interpretan antes de verificarse, lo que permite que se ejecute un flujo de bits malicioso en la estructura lógica de FPGA.

Tomando en cuenta que los ataques se basan en los defectos del protocolo, los investigadores observaron que *«cualquier tipo de cambio no trivial al protocolo de seguridad no es posible sin un rediseño de hardware FPGA y actualmente no está disponible para dispositivos 7-Series y Virtex-6»*.

Además de recomendar a los desarrolladores de hardware que sometan los datos de entrada a la validación criptográfica y hagan uso de un motor de encriptación de flujo de bits parcheado, que ya están en funcionamiento para los dispositivos Zynq-7000, UltraScale+ de Xilinx, se han propuesto una serie de contramedidas, como la implementación de esquemas de ofuscación o parchear la PCB para utilizar los pines de revisión de FPGA para evitar la lectura del registro WBSTAR.

> *«Consideramos esto como un ataque severo, ya que (irónicamente) no existe oportunidad de parchear el silicio subyacente del protocolo criptográfico. Observamos que los 7-Series tienen una parte sustancial del mercado de FPGA, lo que hace que sea aún más difícil o imposible reemplazar estos dispositivos»*, concluyeron los investigadores.