Presse

INFORMATION

PR-Nr. 14 – 15. Januar 2020

Analyse zur Anfälligkeit des ESP32 gegen Fault-Injection-Angriffe

Sicherheitsforscher haben kürzlich einen Fehlerinjektionsangriff auf das ESP32-SoC beschrieben, der zu Einschränkungen der Sicherheit und unbeabsichtigter Offenlegung von Informationen führen kann. Das Security-Design des ESP32 bleibt jedoch für die überwiegende Mehrheit der Espressif-Produkte sicher.

Shanghai (China), 2. Januar 2020

Da nur physisch zugängliche Produkte von einem Fehlerinjektionsangriff betroffen sind, bleibt das Sicherheitsdesign des ESP32 für den überwiegenden Teil des Espressif-Portfolios effektiv sicher.

Für die betroffenen Produkte bietet Espressif einen Migrationspfad, der über eine aktualisierte SoC-Revision (ESP32 ECO V3) verfügbar ist. Bevor jedoch ein Wechsel auf diese Revision vollzogen wird, muss man die Auswirkungen des Angriffs verstehen und beurteilen können, ob die eingesetzten SOCs oder Module tatsächlich einer Gefährdung ausgesetzt sind. Die folgenden Details sollen dabei helfen.

Angriffstaktik

Fehlerinjektionsangriffe zielen auf die Störung des Verhaltens eines elektronischen Systems, indem Fehler auf physikalischem Wege injiziert werden. Ein Angreifer führt einen kleinen Fehler in die extern gesteuerten Komponenten des Chips ein, um dessen normalen Betrieb zu stören. Wenn es speziell auf das Sicherheits-Subsystem abzielt, kann es dazu führen, dass der Angreifer den intern verwendeten kryptografischen Schlüssel erhält oder eine erforderliche Sicherheitsüberprüfung überspringt. Der erhaltene kryptografische Schlüssel kann dann weiterverwendet werden, um Informationen wie Firmware und Daten, die im Flash-Speicher des Geräts gespeichert sind, zu lesen

und zu ändern. Es gibt verschiedene physikalische Methoden für eine Fehlerinjektion wie z. B. sorgfältig zeitgesteuerte Spannungs- oder Taktschwankungen, externe Temperaturschwankungen, Laserbestrahlung oder die Verwendung starker Magnetfelder. Wir glauben, dass diese Art von Angriff nicht nur für ESP32-SoC gilt. Es ist auch bekannt, dass andere kommerzielle Chips für diese Art von Angriff anfällig sind.

Der Angriff auf ESP32, der in dieser Veröffentlichung von LimitedResults siehe (https://limitedresults.com/) beschrieben wurde, führte insbesondere zum:

1. Aufdecken des sicheren Startschlüssels und dadurch Umgehen der Prüfung auf sicheren Start und Starten nicht vertrauenswürdiger Firmware.
2. Aufdecken des Flash-Encryption-Keys, der zum Verschlüsseln der Anwendungsfirmware und des Flash-Inhalts verwendet wurde.

Es ist wichtig, die folgenden Voraussetzungen des Angriffs zu beachten:

1. Der Angriff erfordert physischen Zugriff auf den ESP32-SoC, damit Teile von der Leiterplatte oder dem Modul entfernt werden können. Leiterbahnen müssen möglicherweise auch geschnitten oder modifiziert werden, um sie an das Equipment des Angreifers anzuschließen.
2. Die Störspannungsgeneratoren des Angreifers müssen mit bestimmten Spannungsversorgungspins des SoCs verbunden werden, um damit wiederholte Versuche für zeitrichtige Spannungsschwankungen einzuprägen.

Wie Secure Boot und Flash Encryption im ESP32 funktionieren

Um die Auswirkungen des oben genannten Angriffs zu verstehen, ist es nützlich, sich die beiden genannten Funktionen „Secure Boot“ und „Flash Encryption“ des ESP32 noch einmal vor Augen zu führen:

Secure Boot

Wenn Secure Boot aktiviert ist, generiert und programmiert der Software-Bootloader beim ersten Start einen sicheren Startschlüssel für jedes Gerät im eFUSE-Speicher.

Dies ist der AES-256-Schlüssel, mit dem der Digest für den Software-Bootloader berechnet und der Digest im Flash programmiert wird. Beim anschließenden Start überprüft das bootROM den Digest anhand des tatsächlichen Software-Bootloader-Images mit dem AES-256-Schlüssel.

Die Überprüfung der Anwendung über den Software-Bootloader erfolgt mit dem Elliptic Curve Digital Signature-Algorithmus (ECDSA). Der Software-Bootloader enthält NUR den öffentlichen Schlüssel, während der private Schlüssel bei den Entwicklern verbleibt. Selbst wenn der Software-Bootloader mit einem Fehlerinjektionsangriff entschlüsselt wird, wird nur der öffentliche ECDSA-Schlüssel enttarnt. Es ist nicht möglich, diesen öffentlichen Schlüssel zum Signieren der Firmware oder zum Abrufen des privaten Schlüssels zu verwenden. Daher kann das Gerät nicht mit einer anderen Firmware programmiert werden.

Flash-Verschlüsselung

Wenn die Flash-Verschlüsselungsfunktion aktiviert ist, generiert und programmiert der Software-Bootloader beim ersten Start einen eindeutigen Flash Encryption-Key und verschlüsselt damit die angegebenen Abschnitte der Flash-Daten.

Auswirkung dieses Angriffs auf den ESP32

Mit diesen Informationen zur Funktion des Secure Boot- und Flash-Verschlüsselungsschemas ist es einfach, die Auswirkungen des Verlusts des Flash-Encryption-Keys oder der Umgehung der Secure Boot-Prüfung zu analysieren.

Selbst wenn der Flash-Encryption-Key von einem Angreifer kopiert wird, funktioniert der Flash-Encryption-Key nur auf der Einheit, die der Angreifer verwendet hat. Dies liegt daran, dass jeder ESP32-Chip über einen eindeutig generierten Flash-Encryption-Key verfügt. Der Angreifer kann also nur die Flash-Inhalte und Daten abrufen, die für diese Produkteinheit spezifisch sind.

Genau wie der Flash-Encryption-Key ist auch der sichere Startschlüssel für jeden ESP32-Chip eindeutig. Daher ist die mögliche Umgehung der Prüfung auf sicheren

Systemstart auch für diesen bestimmten ESP32-Chip spezifisch. Dies kann nicht zum Ausführen einer nicht vertrauenswürdigen Anwendung auf einem Remote-ESP32 verwendet werden.

Im Endeffekt ist die Angriffsfläche eines solchen Angriffs aufgrund der geräteindividuellen Flash-Verschlüsselung und der sicheren Boot-Kryptoschlüssel nur auf das spezifische Gerät beschränkt, das der Angreifer besitzt. Dieser Angriff lässt sich nicht auf eine größere Anzahl von Geräten in derselben Produktlinie ausweiten, die sich nicht im physischen Besitz des Angreifers befinden.

Weitere Informationen finden Sie in der Sicherheitsmitteilung vom 1. November 2019.

Wie sind die Auswirkungen auf Produkte im Feld?

Um zu beurteilen, ob ESP32-basierte Produkte möglicherweise von einem solchen Angriff betroffen sind, sind folgende Bedingungen zu prüfen:

- Das Produkt wird im Freien oder an einem öffentlichen Ort eingesetzt, an dem physische Manipulationen und Anschließen von Störgeräten möglich sind.
- Das Produkt enthält ein gemeinsames Geheimnis für alle Produkteinheiten. Dieses Geheimnis ist im Flash-Speicher abgelegt, der mit dem ESP32 verbunden ist.

In diesen Fällen empfehlen wir Ihnen, die neue Version des SoCs zu verwenden.

Wenn das Produkt nicht in eine der oben genannten Kategorien fällt, sind die Auswirkungen des Fault-Injection Angriffs bei Verwendung des aktuellen ESP32-SoC gering.

Wie der neue ESP32 ECO V3 diese Bedrohung adressiert

Der ESP32 ECO V3 verfügt über Verbesserungen, die das Produkt vor Angriffen durch physikalische Fehlerinjektion schützen:

ESP32 ECO V3 unterstützt ein sicheres Startschema auf PKI-Basis (RSA), bei dem die eFuse nur den öffentlichen Schlüssel enthält (tatsächlich einen kryptografischen Hash des öffentlichen Schlüssels) und der private Schlüssel immer beim Firmware-Entwickler bleibt. Auf diese Weise wird sichergestellt, dass kein Angreifer einen sig-

nierten Bootloader erstellen kann, der im Flash beibehalten werden kann und dem Secure Boot fälschlicherweise vertraut.

ESP32 ECO V3 ist gegen Fehlerinjektionsangriffe in Hard- und Software gehärtet, so dass eine unbeabsichtigte Offenlegung von Schlüsseln durch Spannungsstörungen verhindert wird.

Für neue Produktentwicklungen sollten ESP32 ECO V3-basierte Module oder Chips zum Einsatz kommen. Weitere Informationen zu ESP32 ECO V3 finden Sie in der entsprechenden Dokumentation.

Preise und Verfügbarkeit

Samples von ESP32 ECO V3-basierten Modulen (ESP32-WROVER-E und ESP32-WROOM-32E) sind bereits in begrenzter Stückzahl verfügbar. Diese Module werden im März 2020 für die Massenproduktion verfügbar sein. Mehr Informationen zu Preisen und Verfügbarkeit sind unter diesem Kontakt erhältlich.

Email: sales.europe@macnica.com

Kontakt:

Presse
Macnica GmbH
Josef Sigl
Tel. +49-89-899143-0
Email: sales.europe@macnica.com

Sales
Macnica GmbH

Tel. +49-84188198-0
Email: sales.europe@macnica.com

Über Espressif Systems

Espressif Systems (Shanghai) Pte. Ltd. ist ein Fabless-Halbleiterunternehmen mit Sitz im Zhangjiang High-Tech-Park in Shanghai. Das Unternehmen bietet Low-Power-Wi-Fi und Bluetooth-SoCs sowie Wireless-Lösungen für das Internet der Dinge (IoT). Das Unternehmen baut die weit verbreiteten Chips ESP8266 und ESP32 mit einem innovativen Team aus Chip-Design-Spezialisten, Software- und Firmware-Entwicklern und Vermarktern. Espressif ist bestrebt, die besten IoT-Geräte und Softwareplattformen in der Industrie bereitzustellen.

Das Unternehmen unterstützt seine Kunden auch dabei, eigene Lösungen zu entwickeln und sich mit anderen Partnern im IoT-Ökosystem zu vernetzen. Ihre Leidenschaft liegt in der Entwicklung von State-of-the-Art Chipsätzen und ermöglicht es Partnern, großartige Produkte zu liefern. Espressifs Produkte werden in den Bereichen Tablet, OTT-Boxen, Kameras und Internet der Dinge eingesetzt.

Weitere Informationen unter http://www.espressif.com.

Über Macnica Europe GmbH

Macnicas europäischer Hauptsitz wurde ursprünglich 2006 in Großbritannien gegründet und im Juli 2008 nach Deutschland verlegt, um die Wirksamkeit des Service für die europäischen Kunden zu erhöhen.

Durch die Akquisition der Münchner Firma Scantec Mikroelektronik GmbH entstand 2014 eine leistungsfähige Halbleiterdistribution mit Niederlassungen in München und Ingolstadt sowie zahlreichen Vertriebsbüros in Europa und einem attraktiven Portfolio technologisch anspruchsvoller Bauelemente.

Macnica Europe bietet seinen Kunden umfangreichen technischen und logistischen Support, beginnend beim Design-in bis hin zur Produktion über sein globales Service-Netzwerk, unabhängig des endgültigen Bestimmungsorts der Produktlieferung oder der Fertigungsstätte des Kunden.

Über Macnica, Inc.

Macnica wurde 1972 als Unternehmen für die Distribution von Halbleitern mit Hauptsitz in Yokohama, Japan gegründet und verfügt über 65 Vertriebsniederlassungen in Asien, Europa und den USA. Mehr als 2.600 Mitarbeiter sind weltweit beschäftigt und das konsolidierte Jahreseinkommen betrug im Fiskaljahr 2015 ca. 5 Milliarden US$.

Macnica ist bekannt für sein exzellentes Engineering Team mit mehr als 800 Applikationsingenieuren, IC Designern und Software Entwicklern und deren zielgerichtetem Fokus unseren Kunden überdurchschnittliche technische Unterstützung zu bieten. Macnica erweitert kontinuierlich und mit Hilfe strategischer und erfolgreicher Partner die globale Marktpräsenz.