安全公告

Security Advisory

标题/Title	Security Advisory concerning fault injection and ESP32 Flash Encryption & Secure Boot V1 关于故障注入、ESP32 Flash 加密和 Secure Boot V1 的安全公告
发布日期/Issue date	2020-7-20
公告编号/Advisory Number	AR2020-001
编号/Serial Number	CVE-2020-15048 CVE-2020-13629
版本/Version	V1.0

Issue Summary
小结

An attacker who uses fault injection to physically disrupt the ESP32 CPU can bypass the Secure Boot and Flash Encryption physical security features and execute unverified code.
攻击者可以通过“故障注入”攻击，从物理上破坏 ESP32 的 CPU，从而绕过芯片的“安全启动”(Secure Boot) 和 Flash 加密防护，执行未经验证的代码。

These attacks use similar methods and have similar impact to previously advised fault injection issues CVE-2019-15894 and CVE-2019-17391. The vulnerabilities exist in revision 0 and revision 1 of the ESP32 silicon including ESP32-D0WD, ESP32-D2WD, ESP32-S0WD, ESP32-PICO-D4, and modules based on these chips.
此次公告所述漏洞的攻击手段与之前在 CVE-2019-15894 和 CVE-2019-17391 中披露的方法和影响类似。该攻击将主要影响 ESP32 的晶圆版本 0 和 1，包括 ESP32-D0WD，ESP32-D2WD，ESP32-S0WD，ESP32-PICO-D4 以及基于这些芯片的模组产品。

The ESP32-D0WD-V3 and related products (ESP32-D0WDQ6-V3, ESP32-PICO-V3, ESP32-WROOM-32E, ESP32-WROOM-32UE, ESP32-WROOM-32SE, ESP32-WROVER-E, ESP32-WROVER-IE) support a new RSA-based Secure Boot

implementation (ESP32 Secure Boot V2) and have a feature to permanently disable the UART Download Mode via eFuse. Because of these modifications, these attacks can be prevented on ESP32 V3 SoCs and modules.
ESP32-D0WD-V3 及相关产品（ESP32-D0WDQ6-V3、ESP32-PICO-V3、ESP32-WROOM-32E、ESP32-WROOM-32UE、ESP32-WROOM-32SE、ESP32-WROVER-E、ESP32-WROVER-IE）支持新的基于 RSA 的“安全启动”功能（即 ESP32 Secure Boot V2），并可以通过 eFuse 永久禁用 UART 下载模式，因此不在本次披露攻击的影响范围内。

Similarly, these attacks do not apply to ESP32-S2 or newer SoCs.
同样地，ESP32-S2 及以后的芯片也不存在上述问题。

These issues have been found and disclosed to Espressif by researchers Niek Timmers and Cristofaro Mune of Raelize. Espressif thanks the researchers for responsibly disclosing these issues.
该问题由 Raelize 的研究人员 Niek Timmers 和 Cristofaro Mune 发现，并向乐鑫披露。乐鑫感谢这些研究人员负责任地披露了此次问题。

What is Fault Injection?
了解故障注入攻击

Fault injection is a technique for disrupting the behavior of a hardware system by injecting faults via physical means, often by carefully timed voltage or clock fluctuations. To deploy fault injection an attacker must have physical access to the hardware to modify it and inject faults.
故障注入是一种通过物理方式注入故障来破坏硬件系统行为的技术，这些方式通常是通过精准定时的电压或时钟波动。要实现故障注入，攻击者必须具有对硬件的物理访问权限才能对其进行修改并注入故障。

Following a fault, the system will usually crash. However sometimes a carefully timed fault may cause the CPU or an internal hardware process to skip an instruction or corrupt the result of an operation. By repeating the fault injection procedure many times, an attacker may eventually get a result which bypasses a security measure.
故障注入后，系统通常会崩溃。但是，有时一个精准定时的故障也可能会导致 CPU 跳过特定指令或者破坏特定计算结果。通过大量重复故障注入的过程，攻击者最终可能会绕过安全措施。

All electronic hardware is vulnerable to some types of physical fault injection, although the difficulty of inducing the fault varies.
尽管引发故障的难度各不相同，但所有电子设备都容易受到某些类型的物理故障注入的影响。

For more information about the impact of fault injection, see the Espressif Fault Injection Impact Analysis article from January 2020. The attacks described in this advisory have similar impact.
有关故障注入影响的更多信息，请参阅乐鑫 2020 年 1 月发表的故障注入影响分析文章。此文章中描述的攻击具有类似的影响。

Details of CVE-2020-15048
CVE-2020-15048 相关内容

By manipulating ciphertext of encrypted flash connected to an ESP32, an attacker using CVE-2020-15048 can repeatedly read two (effectively random) 32-bit plaintext values which are printed to the serial console during the normal ESP32 ROM boot process. If this process is repeated enough times, ciphertext matching a chosen 32-bit plaintext address in mask ROM can be found and the attacker can use a fault injection attack to bypass normal execution flow and execute from this address.
在 CVE-2020-15048 描述的攻击手段中，攻击者可以通过篡改与 ESP32 相连的加密 flash 中的密文，在 ESP32 芯片 ROM 的正常启动过程中，重复读取到打印到串口控制台（serial console）的两个（有效随机的) 32 位明文值。这样，攻击者即可以在掩码 ROM 中找到与选择的 32 位明文地址相匹配的密文，并可能使用故障注入攻击，绕过正常的执行程序流，并从该地址开始启动。

This technique requires an exhaustive search for a suitable 32-bit value, before the fault injection attack is possible. The attacker receives two random “guesses” per boot attempt. The researchers who reported this vulnerability estimated that without further optimization of the search process this search would take over thirteen years to complete on a single device. Nevertheless, this constitutes a reduction of the specified 256-bit Flash encryption key strength.
攻击者必须进行大量的搜索，才能找到一个合适的 32 位明文，从而进行故障注入攻击。攻击者在芯片每启动一次时可以“猜”两次。根据本问题披露者的估计，如果不继续优化攻击手段，照此速度计算，攻击者必须花费 13 年时间才能破解一部设备。尽管如此，这仍然会削弱 256 位 Flash 加密密钥的强度。

Details of CVE-2020-13629
CVE-2020-13629 相关内容

By writing attacker-controlled data to SRAM using the UART Download Mode and then triggering a system reset into normal boot mode, an attacker can seed uninitialized memory with values that are not read during normal boot execution. By then carrying out a fault injection attack the attacker can cause the CPU to execute an attacker-controlled address previously written to SRAM.
攻击者通过在 UART 下载模式下将控制数据写入 SRAM，然后触发系统重置到正常 boot 模式，从而在未初始化的内存中植入芯片在正常启动执行期间不会读取的值。借助这样的故障注入，CPU 会执行一段之前被控制者写入 SRAM 的地址。

Related Findings
相关阅读

The researchers who reported CVE-2020-15048 and CVE-2020-13629 findings simultaneously reported results from additional fault injection research.
报告 CVE-2020-15048 和 CVE-2020-13629 的研究人员同时也报告了来自其他故障注入研究的结果。

Espressif assessed these related reports used a new method for injecting the fault, but were otherwise equivalent to the already disclosed CVE-2019-15894 and CVE-2019-17391, and/or required the ESP32 to be configured using a configuration already documented as insecure. For this reason, Espressif only acted on the reports relating to CVE-2020-15048 and CVE-2020-13629.
经过评估，乐鑫认为其他报告中虽然采用了不同的故障注入手段，但实质与 CVE-2019-15894 与 CVE-2019-17391 中的披露内容一致，或需使用并非进行充分安全配置的 ESP32。因此，乐鑫目前仅针对 CVE-2020-15048 和 CVE-2020-13629 的相关报告作出有关回应。

Espressif is grateful to the researchers for providing their comprehensive findings under a responsible disclosure process.
乐鑫感谢研究人员在负责任的披露过程下，也提供了他们的全面发现。

Other Espressif Products
其他乐鑫产品

ESP32 V3 RSA-based Secure Boot V2 and newer Espressif SoCs use a different boot process and a different Secure Boot verification method. The Secure Boot V2 boot process is not vulnerable to these attacks.
ESP32 V3 芯片采用基于 RSA 加密算法的安全启动 V2 版本，其他更新款的芯片采用了不同的启动方式和不同的安全启动验证手段。安全启动 V2 版本不易受到这些攻击影响。

ESP32 V3 and newer Espressif SoCs also have eFuse bits which can be programmed to permanently disable UART Download Mode. In the case that this eFuse is programmed, it is not possible for the attacker to boot into UART Download Mode and write data to SRAM as required for CVE-2020-13629.
ESP32 V3 和 ESP32-S2 系列芯片可以通过配置 eFuse 位，永久禁用 UART 下载模式。因此，如果已经通过 eFuse 位永久禁用了 UART 下载模式，则攻击者将无法使芯片进入 UART 下载模式，向 SRAM 写入数据，并完成 CVE-2020-13629 中描述的攻击。

Recommendations for ESP32 Users
对 ESP32 用户的建议

Because of similarities to previously disclosed fault injection attacks, similar recommendations continue to apply for ESP32 users.
由于本次披露的故障注入攻击与之前的披露很类似，因此之前提供给 ESP32 用户的建议本披露仍然适用。

If producing devices which require ESP32 Flash Encryption and/or Secure Boot features then it is recommended to use ESP32-D0WD-V3 chips or the related V3 modules which include fault injection checks in ROM. Please contact Espressif Sales with your requirements.
如果您的产品需要使用 ESP32 的 Flash 加密和/或安全启动功能，那么建议使用 ESP32-D0WD-V3 芯片或相关的 V3 芯片/模组，此类芯片/模组已在 ROM 中增加了针对故障注入的检查。如有需求，请与乐鑫销售团队联系。

For already deployed hardware using ESP32 silicon revisions 0 and 1, there is no software mitigation for this issue.
对于目前芯片晶圆版本为 0 和 1 的 ESP32 硬件，目前暂时无法通过软件手段解决该问题。

Users of ESP32 V3 silicon:
对 ESP32 晶圆版本 3 芯片用户的建议:

1) Should migrate from Secure Boot V1 to the RSA-based Secure Boot V2 for new devices. Support for the new Secure Boot is enabled in ESP-IDF V4.1 and newer.
1) 请升级设备固件至 ESP-IDF V4.1 或以上版本，将设备的安全启动（Secure Boot ）程序从 V1 升级至到基于 RSA 加密算法的 V2 版本。

2) If it is not needed, users should permanently disable UART Download Mode in production devices. Support for burning the corresponding eFuse bit automatically will be available in ESP-IDF versions V3.3.3, V4.0.2, V4.1.1, V4.2 and newer. Disabling UART Download Mode can be done via OTA update for devices already deployed in the field.
2) 如非必要，用户应永久禁用 UART 下载模式。目前在 ESP-IDF版本 V3.3.3、V4.0.2、V4.1.1、V4.2 及更新版本中将支持自动配置 eFuse 位禁用 UART 下载模式。此外，部署至终端已经量产的设备，也可以通过 OTA 空中升级，禁用 UART 下载模式。

Additional Recommendations
其他建议

Remove any unnecessary sensitive data from flash storage, if possible. This includes providing a “factory reset” option which removes customer data from flash before the product is sold or disposed of.
如果可能的话，请从 Flash 闪存中删除任何非必要的敏感数据。此外，还可以提供“恢复出厂设置”选项，允许产品在售出或弃用前删除 Flash 中的客户数据。

Use per-device unique keys for Secure Boot and Flash Encryption.
每个设备的安全启动和 Flash 加密功能均应使用唯一的密钥。

Generate per-device unique keys stored in flash for application uses, rather than using a single shared key across all devices.
请为每个设备生成唯一密钥，存储在 flash 中供应用程序使用。不同设备不要采用相同的密钥。