مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Critical Vulnerabilities in U-Boot

Tracking #:432319278

Date:10-07-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities have been identified in U-Boot (Das U-Boot) bootloader, a widely used open-source bootloader deployed in embedded devices, IoT platforms, networking equipment, and Baseboard Management Controllers (BMCs).

TECHNICAL DETAILS:

Multiple critical vulnerabilities have been identified in U-Boot (Das U-Boot) bootloader, a widely used open-source bootloader deployed in embedded devices, IoT platforms, networking equipment, and Baseboard Management Controllers (BMCs).
The vulnerabilities affect U-Boot's Verified Boot implementation, specifically the Flattened Image Tree (FIT) image parsing and signature verification process. Successful exploitation could allow attackers to execute arbitrary code before authentication controls are applied or cause devices to become unavailable through denial-of-service (DoS) conditions.
The flaws are triggered when U-Boot processes specially crafted malicious FIT images before completing cryptographic signature validation. Since U-Boot executes before the operating system and is responsible for establishing the firmware trust chain, exploitation could compromise the integrity of the entire boot process.
Organizations using devices based on affected U-Boot versions, particularly those supporting remote firmware updates through management interfaces such as BMCs, should prioritize applying vendor-provided security updates.

Vulnerability Details:

- BRLY-2026-037
  - Severity: Critical
  - Issue: Null pointer dereference and potential stack-based buffer overflow in fdt_find_regions during FIT image signature verification.
  - Impact: May allow memory corruption and potential arbitrary code execution before authentication.
- BRLY-2026-038
  - Severity: Critical
  - Issue: Stack buffer underflow caused by negative length values returned from failed fdt_get_name operations.
  - Impact: Could corrupt stack memory and potentially enable pre-authentication code execution.
- BRLY-2026-039
  - Severity: High
  - Issue: Improper validation of hashed-strings property size values.
  - Impact: Allows out-of-bounds reads, potentially causing system crashes during FIT image verification.
- BRLY-2026-040
  - Severity: High
  - Issue: NULL pointer dereference when fdt_get_property_by_offset returns NULL for older FDT formats.
  - Impact: May trigger denial-of-service conditions during boot verification.
- BRLY-2026-041
  - Severity: High

- Issue: Insufficient validation of external FIT image data properties (data-position, data-offset, and data-size).
- Impact: Attackers may cause out-of-bounds memory access leading to device crashes.

- BRLY-2026-042
  - Severity: High
  - Issue: Unbounded recursion in fdt_check_no_at during FIT format validation.
  - Impact: Deeply nested malicious FIT images can exhaust stack memory and cause denial-of-service.

Technical Details

- The vulnerabilities exist within the FIT image parsing and verification logic of U-Boot.
- Exploitation occurs before signature verification is fully completed, allowing malformed images to influence memory operations.
- Two vulnerabilities (BRLY-2026-037 and BRLY-2026-038) can potentially be chained to corrupt stack memory and overwrite return addresses.
- Four vulnerabilities (BRLY-2026-039 through BRLY-2026-042) primarily result in denial-of-service conditions.
- A successful attack may prevent affected devices from booting normally, requiring recovery actions such as firmware reflashing.

RECOMMENDATIONS:

- **Apply Security Updates**
  - Update U-Boot to the latest patched release containing fixes for the affected vulnerabilities.
- **Update Device Firmware**
  - Apply firmware updates from device manufacturers for affected routers, IoT devices, embedded systems, and BMC platforms.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.binarly.io/blog/unfit-to-boot-breaking-u-boots-fit-signature-verification