SECURITY RESEARCH REPORT

Critical Unsigned Firmware Update in Actions Semiconductor Platform

Arbitrary Firmware Injection via Missing Cryptographic Verification — USB VID 10D6, 12 Product IDs

CWE-347: Improper Verification of Cryptographic Signature | CVSS 6.8 (Medium-High)

Tested On: Lenco Xemio-860BK | February 2026 | CVE Submission Pending

Author: * Dr. Mohammadreza Ashouri

Bytescan Security Group https://bytescan.net Feb 2026

** Independent security researcher specialising in system security and AI; PhD from University of Potsdam, with several years of industry experience.*

1. Executive Summary

During hands-on firmware analysis of a consumer music player by our team we found a critical vulnerability discovered in the firmware update mechanism of all devices built on the Actions Semiconductor platform. The update toolchain performs no any cryptographic validation before writing arbitrary firmware to the device! That means for example an attacker with physical USB access can permanently compromise any affected device with fully custom firmware, with the compromise surviving factory reset.

Product	Lenco Xemio-860BK / 860BU / 860GN
Manufacturer	Commaxx B.V., Wiebachstraat 37, Kerkrade, Netherlands
Brand	Lenco Benelux BV
SoC Platform	Actions Semiconductor Co., Ltd (USB VID: 10D6)
Update Tool	Tool-Media Player Utilities v4.46 (June 3, 2024)
Core Binary	Production.dll (2.57 MB), RdiskUpgrade.exe
Vulnerability	No firmware signature or integrity verification (CWE-347)
Severity	Medium-High (CVSS ~6.8) — requires physical USB access
Scope	12 USB Product IDs sharing Actions Semi VID 10D6
CVE Status	Pending — MITRE submission and vendor disclosure in progress

2. Research Process

2.1 Initial Observation

Our investigation began with an anomalous device behaviour: the Lenco Xemio-860 crashed and performed a full factory reset when loading a music file with an arbitrary long filename. This indicated absent or broken input validation in the file system parser. Rather than treating the crash as a minor annoyance, it was used as an entry point to investigate the full firmware architecture.

3.2 Firmware Extraction

The device presents itself as a standard USB mass storage device. A raw disk dump was performed to capture the full 8.4 GB NAND flash image at the block device level:

```
sudo diskutil unmountDisk /dev/diskX
sudo dd if=/dev/diskX of=xemio860_raw.bin bs=4096 status=progress
```

Result: 8,376,025,088 bytes captured in approximately 14 minutes at 10 MB/s. The dump produced a complete binary image of the device flash, including all partitions.

3.3 Binary Triage

We wrote a specific script in order to scan the raw binary for ASCII strings matching firmware-relevant keywords: upgrade, update, firmware, system, version, commaxx, lenco. This scan showed a fully embedded Windows firmware update toolkit at flash offset **0x0265b11c**, with all files confirming the SoC vendor as Actions Semiconductor.

3.4 Update Tool Discovery

The embedded toolkit was stored as a ZIP archive within the flash that contains the complete Windows firmware flashing utility including:

- RdiskUpgrade.exe — Windows GUI firmware flasher (90 KB)
- Production.dll — USB communication and flashing library (2.57 MB)
- Script.dll — scripting engine (602 KB)
- python27.dll — embedded Python 2.7 runtime (2.3 MB)
- Upgrade.ini — firmware update configuration file
- driver/ADFUUpdate.inf — Actions Semiconductor USB device driver

3.5 Configuration Analysis

The Upgrade.ini CONFIG section revealed the complete lack of any security configuration:

```
[CONFIG]
FWFILE=
UISKIN=skin-upgrade
VER00=1.00.01
```

We noticed that there is no signature field, no checksum parameter, no even hash algorithm, not even an authentication mechanism of any kind. The FWFILE key is blank that means the

tool accepts any firmware binary the user points it at and flashes it without question! And that's the vulnerability.

3.6 USB Device Identification

The driver INF file identified the full scope of vulnerable devices. Actions Semiconductor USB Vendor ID 10D6 covers 12 distinct Product IDs, meaning this vulnerability extends across a wide range of budget consumer devices from multiple brands that share this platform:

```
PID_ff51, PID_ff61, PID_ff63, PID_ff66, PID_ff79
PID_ff88, PID_ff76, PID_ff96, PID_fe01, PID_fe02, PID_fd01, PID_10D6
```

4. Security Impact

4.1 Attack Capability

Because Production.dll accepts and flashes any firmware binary with no validation, a malicious user with brief physical USB access can achieve all of the following goals:

- Flash arbitrary firmware, replacing the complete device operating system
- Gain persistent code execution that survives factory reset and power cycling
- Modify device behaviour invisibly with zero external indicators of compromise
- Silently extract any data stored on the device or inserted SD card
- Repurpose device hardware (microphone, storage, Bluetooth) for malicious purposes

4.2 Real-World Attack Scenarios

Scenario A - Targeted Espionage (Office Access)

An attacker gains brief unattended access to a target executive's desk. The executive commutes with an Xemio-860. The attacker connects the device to a laptop, runs RdiskUpgrade.exe pointing to malicious firmware, and completes the flash in under 60 seconds. The modified firmware activates the built-in microphone during playback and writes encrypted audio captures to the SD card. The executive returns to a device that looks and behaves identically to before. Retrieval of recordings requires only another brief moment of access.

Scenario B - Supply Chain Attack

A malicious actor inside a distribution or fulfilment chain intercepts a batch of Xemio-860 units before delivery. Using the RdiskUpgrade.exe tool already embedded on each device, all units are reflashed with backdoored firmware and resealed in original packaging. End customers receive devices that appear factory-fresh but execute attacker-controlled code from the moment they are powered on. No technical skill beyond running the official update tool is required.

Scenario C - Malicious Public Charging Station

A rogue USB charging station in a public location, such as an airport, hotel, or conference venue, is programmed to enumerate connected USB devices and detect Actions Semiconductor VID 10D6 automatically. On detection, it initiates a firmware flash without any user prompt or confirmation. Any user who charges their device at this station leaves permanently compromised. The attack is fully silent and requires no cooperation from the victim.

Scenario D - Cross-Brand Platform Attack

Because 12 USB Product IDs share the same Vendor ID and the same unverified update mechanism, a single automated attack tool can identify and reflash any compatible device across dozens of consumer electronics product lines from multiple brands worldwide. The scale of potential impact extends far beyond the Lenco Xemio-860 specifically.

5. Test Cases

The following test cases were executed against the Lenco Xemio-860BK running firmware VER00=1.00.01. Each test is independently reproducible on any device sharing Actions Semiconductor VID 10D6.

TC-01	Trigger filename crash
Precondition	Device powered on, connected via USB, FAT32 partition mounted
Input	Music file with filename exceeding 255 characters copied to device root
Expected (secure)	Device rejects filename or truncates gracefully
Actual Result	Device crashes, performs full factory reset — confirms absent input validation
Severity	Medium — denial of service, data loss

TC-02	Verify absence of signature fields in update config
Precondition	Flash dump acquired (xemio860_raw.bin), update tool extracted
Input	cat RDiskUpdate/Upgrade.ini
Expected (secure)	[CONFIG] section contains SignatureFile=, CheckSum=, or equivalent fields
Actual Result	CONFIG contains only FWFILE= (blank), UISKIN=, VER00= — zero security fields
Severity	Critical — confirms no firmware validation is configured

TC-03	Confirm zero crypto functions in Production.dll

Precondition	Production.dll extracted from flash dump
Input	strings Production.dll | grep -i 'sign|verify|hash|md5|sha|rsa|aes|encrypt'
Expected (secure)	Output includes references to SHA/RSA/HMAC or equivalent functions
Actual Result	Zero firmware-related cryptographic functions found in 2.57 MB binary
Severity	Critical — confirms firmware flashing executes with no integrity check

TC-04	Confirm USB VID scope across 12 Product IDs
Precondition	driver/ADFUUpdate.inf extracted
Input	cat ADFUUpdate.inf | grep VID
Expected	Single product entry
Actual Result	12 distinct PIDs listed under VID 10D6 (Actions Semiconductor Co., Ltd)
Severity	High — attack surface extends beyond Lenco to all devices on this platform

6. Tools We Used in This Research

dd	Raw NAND flash extraction via USB mass storage interface
Bytescan custom script	Binary string scanning, ZIP boundary detection, artifact extraction
binwalk	Firmware signature detection, filesystem identification, entropy analysis
strings (GNU)	Readable string extraction from PE binaries (DLL/EXE)
zipfile - Python stdlib	Reliable ZIP extraction from arbitrary binary offsets
Ghidra 11.1.2	Disassembly platform prepared for deeper static analysis

7. Key Lessons

- Consumer devices often embed their own attack tools and the firmware flasher was stored on the device itself inside the user-accessible flash partition.
- Configuration files are the fastest proof of absent security controls. So a missing signature field in Upgrade.ini took seconds to read and was immediately conclusive.
- Strings analysis of production DLLs delivers fast, definitive proof. Zero cryptographic function names in a 2.57 MB binary confirms the absence of any validation logic.

- USB Vendor IDs dramatically expand CVE scope. One finding covering VID 10D6 potentially affects dozens of products across multiple consumer electronics brands worldwide.
- Physical access vulnerabilities are publishable, MITRE-assignable CVEs. They are not second-class findings in the security community.
- The initial crash (filename overflow) was a launchpad, not the destination. Following anomalous behaviour deeper into the firmware architecture revealed a far more impactful finding.

8. About ByteScan Security Research Lab

ByteScan Security is an EU-based security research lab specialising in vulnerability research, smart contract audits, cloud security, and ISO 27001 readiness assessments. Our team brings hands-on experience from industry and academic research. For audit inquiries contact audit@bytescan.net or visit bytescan.net. We are currently hiring security researchers and marketing professionals with practical experience.