# CVE Detail – CVE-2022-30273

The Motorola MDLC protocol through 2022-05-02 mishandles message integrity. It supports three security modes: Plain, Legacy Encryption, and New Encryption. In Legacy Encryption mode, traffic is encrypted via the Tiny Encryption Algorithm (TEA) block-cipher in ECB mode. This mode of operation does not offer message integrity and offers reduced confidentiality above the block level, as demonstrated by an ECB Penguin attack against any block ciphers.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.31818

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-327: Use of a Broken or Risky Cryptographic Algorithm
* CWE-345: Insufficient Verification of Data Authenticity

## CAPEC(s)

* CAPEC-111: JSON Hijacking (aka JavaScript Hijacking)
* CAPEC-141: Cache Poisoning
* CAPEC-142: DNS Cache Poisoning
* CAPEC-148: Content Spoofing
* CAPEC-20: Encryption Brute Forcing
* CAPEC-218: Spoofing of UDDI/ebXML Messages
* CAPEC-384: Application API Message Manipulation via Man-in-the-Middle
* CAPEC-385: Transaction or Event Tampering via Application API Manipulation
* CAPEC-386: Application API Navigation Remapping
* CAPEC-387: Navigation Remapping To Propagate Malicious Content
* CAPEC-388: Application API Button Hijacking
* CAPEC-459: Creating a Rogue Certification Authority Certificate
* CAPEC-473: Signature Spoof
* CAPEC-475: Signature Spoofing by Improper Validation
* CAPEC-608: Cryptanalysis of Cellular Encryption
* CAPEC-614: Rooting SIM Cards
* CAPEC-665: Exploitation of Thunderbolt Protection Flaws
* CAPEC-701: Browser in the Middle (BiTM)
* CAPEC-97: Cryptanalysis

## ATT&CK Techniques

* T1553.002: Code Signing
* T1491: Defacement
* T1542.002: Component Firmware
* T1036.001: Invalid Code Signature
* T1584.002: DNS Server
* T1557.002: ARP Cache Poisoning
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* TrickBot (malware)
* BLINDINGCAN (malware)
* Stuxnet (malware)
* WindTail (malware)
* StrongPity (malware)
* Janicab (malware)
* Ecipekac (malware)
* NETWIRE (malware)
* GreyEnergy (malware)
* Regin (malware)
* CHIMNEYSWEEP (malware)
* BOOSTWRITE (malware)
* SpicyOmelette (malware)
* LockerGoga (malware)
* Anchor (malware)
* Lumma Stealer (malware)
* Epic (malware)
* Gazer (malware)
* Metamorfo (malware)
* Bandook (malware)
* PipeMon (malware)
* Black Basta (malware)
* ZeroCleare (malware)
* RTM (malware)
* StrelaStealer (malware)
* GoBear (malware)
* Bazar (malware)
* HermeticWiper (malware)
* Cobalt Strike (malware)
* SUNBURST (malware)
* Cyclops Blink (malware)
* Daserf (malware)
* MacMa (malware)
* ROADSWEEP (malware)
* More\_eggs (malware)
* SysUpdate (malware)
* BackConfig (malware)
* Nerex (malware)
* Kessel (malware)
* Clop (malware)
* Troll Stealer (malware)
* Ebury (malware)
* ChChes (malware)
* AppleJeus (malware)
* BADNEWS (malware)
* QakBot (malware)
* Gelsemium (malware)
* Helminth (malware)
* HermeticWizard (malware)
* SILENTTRINITY (tool)
* PcShare (tool)
* CSPY Downloader (tool)
* QuasarRAT (tool)
* LuminousMoth (intrusion-set)
* Wizard Spider (intrusion-set)
* FIN7 (intrusion-set)
* Velvet Ant (intrusion-set)
* APT41 DUST (campaign)
* ArcaneDoor (campaign)
* OilRig (intrusion-set)
* Equation (intrusion-set)
* SolarWinds Compromise (campaign)
* Lazarus Group (intrusion-set)
* Daggerfly (intrusion-set)
* TA505 (intrusion-set)
* Suckfly (intrusion-set)
* FIN6 (intrusion-set)
* Silence (intrusion-set)
* Patchwork (intrusion-set)
* APT28 (intrusion-set)
* Darkhotel (intrusion-set)
* Operation Honeybee (campaign)
* Kimsuky (intrusion-set)
* Leviathan (intrusion-set)
* LAPSUS$ (intrusion-set)
* RedDelta Modified PlugX Infection Chain Operations (campaign)
* menuPass (intrusion-set)
* Moses Staff (intrusion-set)
* Operation Dream Job (campaign)
* Molerats (intrusion-set)
* APT37 (intrusion-set)
* APT41 (intrusion-set)
* FIN13 (intrusion-set)
* GALLIUM (intrusion-set)
* C0015 (campaign)
* Winnti Group (intrusion-set)
* Saint Bear (intrusion-set)
* Scattered Spider (intrusion-set)
* Windshift (intrusion-set)
* Sea Turtle (intrusion-set)
* Cleaver (intrusion-set)
* CopyKittens (intrusion-set)
* PROMETHIUM (intrusion-set)

## Affected Products

* cpe:2.3:a:motorolasolutions:mdlc:4.80.0024:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:motorolasolutions:mdlc:4.82.004:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:motorolasolutions:mdlc:4.83.001:\*:\*:\*:\*:\*:\*:\*