# CVE Detail – CVE-2022-30272

The Motorola ACE1000 RTU through 2022-05-02 mishandles firmware integrity. It utilizes either the STS software suite or ACE1000 Easy Configurator for performing firmware updates. In case of the Easy Configurator, firmware updates are performed through access to the Web UI where file system, kernel, package, bundle, or application images can be installed. Firmware updates for the Front End Processor (FEP) module are performed via access to the SSH interface (22/TCP), where a .hex file image is transferred and a bootloader script invoked. File system, kernel, package, and bundle updates are supplied as RPM (RPM Package Manager) files while FEP updates are supplied as S-rec files. In all cases, firmware images were found to have no authentication (in the form of firmware signing) and only relied on insecure checksums for regular integrity checks.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.19209

## CVSS Scoring

CVSS v3.1 Score: 7.2

Severity: HIGH

## Mapped CWE(s)

* 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-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-665: Exploitation of Thunderbolt Protection Flaws
* CAPEC-701: Browser in the Middle (BiTM)

## ATT&CK Techniques

* T1491: Defacement
* T1542.002: Component Firmware
* T1584.002: DNS Server
* T1557.002: ARP Cache Poisoning
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* LuminousMoth (intrusion-set)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* LAPSUS$ (intrusion-set)
* FIN13 (intrusion-set)
* Sea Turtle (intrusion-set)
* Cleaver (intrusion-set)

## Affected Products

* cpe:2.3:o:motorola:ace1000\_firmware:-:\*:\*:\*:\*:\*:\*:\*