# CVE Detail – CVE-2022-30271

The Motorola ACE1000 RTU through 2022-05-02 ships with a hardcoded SSH private key and initialization scripts (such as /etc/init.d/sshd\_service) only generate a new key if no private-key file exists. Thus, this hardcoded key is likely to be used by default.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.28213

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-259: Use of Hard-coded Password
* CWE-798: Use of Hard-coded Credentials

## CAPEC(s)

* CAPEC-191: Read Sensitive Constants Within an Executable
* CAPEC-70: Try Common or Default Usernames and Passwords

## ATT&CK Techniques

* T1078.001: Default Accounts
* T1552.001: Credentials In Files

## Used By (Actors/Tools)

* TrickBot (malware)
* Stuxnet (malware)
* Smoke Loader (malware)
* HyperStack (malware)
* Emotet (malware)
* Hildegard (malware)
* BlackEnergy (malware)
* XTunnel (malware)
* pngdowner (malware)
* StrelaStealer (malware)
* Pysa (malware)
* Agent Tesla (malware)
* jRAT (malware)
* Azorult (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* LaZagne (tool)
* Pupy (tool)
* QuasarRAT (tool)
* Indrik Spider (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* TA505 (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* Leafminer (intrusion-set)
* Magic Hound (intrusion-set)
* MuddyWater (intrusion-set)
* Kimsuky (intrusion-set)
* FIN13 (intrusion-set)
* Scattered Spider (intrusion-set)
* RedCurl (intrusion-set)
* Leviathan Australian Intrusions (campaign)
* APT3 (intrusion-set)
* HomeLand Justice (campaign)
* APT33 (intrusion-set)

## Affected Products

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