# CVE Detail – CVE-2012-3503

The installation script in Katello 1.0 and earlier does not properly generate the Application.config.secret\_token value, which causes each default installation to have the same secret token, and allows remote attackers to authenticate to the CloudForms System Engine web interface as an arbitrary user by creating a cookie using the default secret\_token.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.78865

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* 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:a:theforeman:katello:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:redhat:enterprise\_linux\_server:6.0:\*:\*:\*:\*:\*:\*:\*