# CVE Detail – CVE-2018-3825

In Elastic Cloud Enterprise (ECE) versions prior to 1.1.4 a default master encryption key is used in the process of granting ZooKeeper access to Elasticsearch clusters. Unless explicitly overwritten, this master key is predictable across all ECE deployments. If an attacker can connect to ZooKeeper directly they would be able to access configuration information of other tenants if their cluster ID is known.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.33272

## CVSS Scoring

CVSS v3.0 Score: 5.9

Severity: MEDIUM

## Mapped CWE(s)

* CWE-1188: Initialization of a Resource with an Insecure Default
* CWE-321: Use of Hard-coded Cryptographic Key

## CAPEC(s)

* CAPEC-665: Exploitation of Thunderbolt Protection Flaws

## ATT&CK Techniques

* T1542.002: Component Firmware
* T1556: Modify Authentication Process
* T1211: Exploitation for Defense Evasion

## Used By (Actors/Tools)

* Cyclops Blink (malware)
* Kessel (malware)
* Ebury (malware)
* SILENTTRINITY (tool)
* Velvet Ant (intrusion-set)
* ArcaneDoor (campaign)
* Equation (intrusion-set)
* APT28 (intrusion-set)
* FIN13 (intrusion-set)

## Affected Products

* cpe:2.3:a:elastic:elastic\_cloud\_enterprise:\*:\*:\*:\*:\*:\*:\*:\*