# CVE Detail – CVE-2009-0255

The System extension Install tool in TYPO3 4.0.0 through 4.0.9, 4.1.0 through 4.1.7, and 4.2.0 through 4.2.3 creates the encryption key with an insufficiently random seed, which makes it easier for attackers to crack the key.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.89388

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-330: Use of Insufficiently Random Values

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-485: Signature Spoofing by Key Recreation
* CAPEC-59: Session Credential Falsification through Prediction

## ATT&CK Techniques

* T1552.004: Private Keys
* T1110: Brute Force

## Used By (Actors/Tools)

* Machete (malware)
* Mafalda (malware)
* Hildegard (malware)
* Chaos (malware)
* FoggyWeb (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Troll Stealer (malware)
* Ebury (malware)
* Kinsing (malware)
* QakBot (malware)
* jRAT (malware)
* AADInternals (tool)
* Empire (tool)
* PoshC2 (tool)
* Mimikatz (tool)
* CrackMapExec (tool)
* Operation Wocao (campaign)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* SolarWinds Compromise (campaign)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* TeamTNT (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* Volt Typhoon (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Rocke (intrusion-set)
* Scattered Spider (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:a:typo3:typo3:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:typo3:typo3:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:typo3:typo3:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:4.0:\*:\*:\*:\*:\*:\*:\*