# CVE Detail – CVE-2020-27020

Password generator feature in Kaspersky Password Manager was not completely cryptographically strong and potentially allowed an attacker to predict generated passwords in some cases. An attacker would need to know some additional information (for example, time of password generation).

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## EPSS

EPSS Score: N/A

Percentile: 0.49799

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-326: Inadequate Encryption Strength

## CAPEC(s)

* CAPEC-112: Brute Force
* CAPEC-192: Protocol Analysis
* CAPEC-20: Encryption Brute Forcing

## ATT&CK Techniques

* T1110: Brute Force

## Used By (Actors/Tools)

* Chaos (malware)
* Caterpillar WebShell (malware)
* Pysa (malware)
* Kinsing (malware)
* QakBot (malware)
* PoshC2 (tool)
* CrackMapExec (tool)
* Dragonfly (intrusion-set)
* OilRig (intrusion-set)
* Fox Kitten (intrusion-set)
* Turla (intrusion-set)
* Ember Bear (intrusion-set)
* APT28 (intrusion-set)
* HEXANE (intrusion-set)
* 2016 Ukraine Electric Power Attack (campaign)
* APT39 (intrusion-set)
* APT38 (intrusion-set)
* Operation Dream Job (campaign)
* DarkVishnya (intrusion-set)
* APT41 (intrusion-set)
* Agrius (intrusion-set)
* FIN5 (intrusion-set)

## Affected Products

* cpe:2.3:a:kaspersky:password\_manager:\*:\*:\*:\*:\*:windows:\*:\*
* cpe:2.3:a:kaspersky:password\_manager:\*:\*:\*:\*:\*:iphone\_os:\*:\*
* cpe:2.3:a:kaspersky:password\_manager:\*:\*:\*:\*:\*:android:\*:\*
* cpe:2.3:a:kaspersky:password\_manager:9.2:-:\*:\*:\*:windows:\*:\*