# CVE Detail – CVE-2020-25685

A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply\_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.5793

## CVSS Scoring

CVSS v3.1 Score: 3.7

Severity: LOW

## 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:thekelleys:dnsmasq:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:32:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:fedoraproject:fedora:33:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:debian:debian\_linux:10.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:arista:eos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:arista:eos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:arista:eos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:arista:eos:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:arista:eos:\*:\*:\*:\*:\*:\*:\*:\*