RUSTSEC-2020-0001

Stack overflow when resolving additional records from MX or SRV null targets

Reported	January 6, 2020
Issued	October 2, 2020 (last modified: October 19, 2021)
Package	trust-dns-server (crates.io)
Type	Vulnerability
Categories	denial-of-service
Keywords	#stack-overflow #crash
Aliases	CVE-2020-35857
Details	https://github.com/bluejekyll/trust-dns/issues/980
CVSS Score	7.5 HIGH
CVSS Details	

Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Patched	`>=0.18.1`
Unaffected	`<0.16.0`

Description

There's a stack overflow leading to a crash and potential DOS when processing additional records for return of MX or SRV record types from the server.

This is only possible when a zone is configured with a null target for MX or SRV records, i.e. '.'.

Example effected zone record:

```
no-service 86400 IN MX 0 .
```

Prior to 0.16.0 the additional record processing was not supported by trust-dns-server. There Are no known issues with upgrading from 0.16 or 0.17 to 0.18.1. The remidy should be to upgrade to 0.18.1. If unable to do so, MX, SRV or other record types with a target to the null type, should be avoided.