Umbrella-Unterstützung für erweiterte DNS-Fehler

Inhalt

Einleitung

In diesem Dokument wird die Cisco Umbrella-Unterstützung für erweiterte DNS-Fehler beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Umbrella.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Cisco Umbrella hat die vorläufige Unterstützung für Extended DNS Errors (EDE) angekündigt, wie in diesem IETF-Dokument zu Extended DNS Errors definiert.

Die anfängliche Unterstützung von Umbrella konzentriert sich auf DNSSEC-Fehlercodes für SERVFAIL-Antworten. Umbrella plant, in Zukunft Unterstützung für andere Fehlercodes sowie die Textdarstellung der Fehlercodes hinzuzufügen.

Unterstützte Fehlercodes

Code	Name	Unterstützt	Fehler aufgetreten
0	Andere	Nein	
1	Nicht unterstützter DNSKEY-Algorithmus	Ja	DNSKEY-Algorithmus wird nicht unterstützt.
2	Nicht unterstützter DS-Digest-Typ	Ja	Der DS-Digest-Typ wird nicht unterstützt
3	Veraltete Antwort	Nein	
4	Gefälschte Antwort	Nein	
5	DNSSEC unbestimmt	Nein	
6	DNSSEC Bogus	Ja	• Wenn alle relevanten Datensätze gefunden und validiert wurden (Signaturhash stimmt nicht überein) • RRSIG-Signatur/Eigentümerkonflikt • RRSIG ungültig • Negative Beweis ist ungültig NXDOMAIN erwartet gefunden NODATA und umgekehrt • Ein signierter Bereich wurde erreicht, aber kein Delegierungspunkt.
7	Signatur abgelaufen	Ja	RRSIG stimmt mit DNSKEY überein (Keytag und Algorithmus), hat aber eine abgelaufene Signatur
8	Signatur noch nicht gültig	Ja	RRSIG hat DNSKEY (Keytag und Algorithmus) zugeordnet, aber die Signaturanfangszeit liegt hinter dem jetzigen Zeitpunkt.
9	DNSKEY fehlt	Ja	Mit DNSKEY übereinstimmende DS nicht gefunden.
10	RRSIGs fehlen	Ja	RRSIG, der mit dem DNSKEY (Schlüsselwort und Algorithmus) übereinstimmt, wurde nicht gefunden.
11	Kein Zonenschlüsselbitsatz	Ja	Wenn DNSKEY das Zonenbit nicht gesetzt hat.
12	NSEC fehlt	Ja	Negativer Beweis nicht gefunden oder unzureichend.
13	Cache-Fehler	Nein	
14	Nicht bereit	Nein	
15	Gesperrt	Nein	
16	zensiert	Nein	
17	Gefiltert	Nein	
18	Verboten	Nein	

19	Veraltete NXDOMAIN-Antwort	Nein	
20	Nicht autorisierend	Nein	
21	Nicht unterstützt	Nein	
22	Keine erreichbare Autorität	Nein	
23	Netzwerkfehler	Nein	
24	Ungültige Daten	Nein	

Beispielantwort

Eine Abfrage, die einen erweiterten DNS-Fehler zurückgibt, kann den Fehlercode im EDNS-Abschnitt mit dem OPT-Code 15 anzeigen. In dieser Abfrage wird beispielsweise der Fehlercode 6 zurückgegeben, der dem Fehler "DNSSEC Bogus" entspricht:

```
; <<>> DiG 9.11.5-P4-5.1+deb10u1-Debian <<>> +dnssec +nocrypt bogus.d2a10n3.rootcanary.net @m81.sjc.ope
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.