Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

- DNS Flag Day

התאמת שרתי DNS **להרחבת** EDNS

תמצית מנהלים

מסמך זה מתאר מהלך שינוי תצורה אשר יתרחש ב- 1.2.2019 במערכות DNS Resolver. מדובר על מהלך משותף של כל היצרנים המובילים BIND, Knot, Unbound, PowerDNS. אשר יתרחש גם על הרזולברים הפתוחים **Quad 9: 9.9.9.9, Google: 8.8.8.8, CloudFlare: 1.1.1.1** ודומיהם.מהות השינוי היא **ביטול מעקפים** (workarounds) אשר קיימים במערכות הנ"ל, שמטרתם לספק תשובות לשאילתות DNS גם במקרה של time-out הנובע מבעיות ב- EDNS. מהלך **זה נקרא DNS Flag Day.**

EDNS (Extended DNS) הינה הרחבה של פרוטוקול DNS, המאפשרת להעביר בשאילתה מידע נוסף. כיום, resolver שלא מצליח לקבל תשובה לשאילתה עם EDNS, מייצר אותה פעם נוספת, ושולח אותה לשרת האוטוריטטיבי, ללא EDNS. מצב זה מייצר עיכוב בתשובות למשתמשים.

המשמעות של המהלך היא שהחל מ- 1.2.19, מקרה של time-out על שאילתה הכוללת הרחבת EDNS לא יטופל, והיא תיכשל.

מטרת המסמך ליידע את קהילת האינטרנט הישראלי במהלך, ולתת הנחיות כיצד להיערך לשינוי. מי שמפעיל שרת DNS אוטוריטטיבי יצטרך לוודא שפרסום שמות המתחם שבאחריותו ישרוד את השינוי, וימשיך לפעול באופן תקין גם לאחריו.

DNS ו-EDNS– מבוא

פרוטוקול DNS פותח בראשית שנות ה- 80 כמנגנון מבוזר, גלובלי, המתרגם שמות לכתובות IP. נוכח בעיית רוחב הפס שאפיינה את הרשת בשנים האלה, הוחלט באופן טבעי להשתמש ב- UDP כמנגנון להעברת בקשות DNS. פרוטוקול UDP אפשר תקשורת מהירה, אולם תוך הצבת מגבלה על גודל המנות (packets). בשל כך, גודל בקשות DNS הוגבל בזמנו ל- 512 byte. מגבלה זו היוותה חסם לתוספות ושינויים אשר נדרשו בפרוטוקול במרוצת השנים.

בסוף שנות ה- 90 פותח מנגנון אשר איפשר הגדלה של כמות המידע ב- DNS, תוך ווידוא כי הצד השואל והצד העונה תומכים בכך. מנגנון זה נקרא EDNS - Extended DNS, והוא מוגדר ב- RFC 6891 כאן: https://tools.ietf.org/html/rfc6891.

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

EDNS - מהו?

EDNS הינו הרחבה של פרוטוקול DNS המאפשרת להעביר לשרתים אוטוריטטיביים, או לבקש מהם, מידע אודות מגוון נושאים.

הרחבת EDNS מבוססת על הכנסת רשומה ייעודית לשאילתה. מדובר על של רשומת משאב (Resource Record) מסוג חדש, OPT. OPT היא "פסאודו רשומה" (Pseudo RR או Meta RR) אשר הוגדרה במיוחד עבור EDNS. פסאודו רשומות לא נמצאות ב-ZONE של שרת DNS, ולא נשמרות בשום cache. הן נוצרות בעת חילול הבקשות בין resolver לשרת האוטוריטטיבי שאליו הוא פונה.

הרעיון הוא, ששרת DNS אשר לא תומך ב-EDNS, לא יודע מה זה OPT, יתעלם מקיומה של הרשומה ויענה כרגיל. לעומת זאת, שרת שכן תומך בהרחבה, יענה על השאילתה, תוך התייחסות להרחבת ה- EDNS המבוקשת ברשומת OPT.

רשומת OPT מורכבת מ- header ומשתנים שקרויים EDNS options.

Header של רשומת OPT מכיל:

- גרסת ה- EDNS שמבקש הבקשה תומך בה (נכון להיום גרסה 0 בלבד).
- שדה "flags" – נכון להיום משמש רק DNSSEC (יודגם להלן)
- הגודל המקסימלי של המנות (packets), כלומר מעבר ל -512 ועד ל- 4096 , שמבקש הבקשה יכול לתמוך כדי לאפשר את ההרחבה הרצויה.

EDNS options:

כל יתר ההרחבות ממומשות באמצעות משתנים אלה. למשל:

- DNS Cookies
- Client Subnet
- NSID
- וכיוצ"ב.

את הרשימה המלאה ניתן למצוא באתר IANA.

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

דוגמאות:

- ההרחבה הידועה ביותר היא DNSSEC. תפקידה לאפשר אימות של רשומות DNS באמצעות חתימה דיגיטלית. שרת resolver שיודע לפענח DNSSEC, יציין זאת כשהוא מעביר שאילתות לשרתים אוטוריטטיביים. הוא עושה זאת ע"י הפעלת ביט בשדה "*flags*" ב- header של רשומת OPT. שם הביט הוא "do" ומשמעותו DNSSEC OK.

  הפעלת ביט זה היא הודעה לשרת האוטוריטטיבי כי עליו לספק בתשובתו גם מידע DNSSEC (מפתחות, חתימות וכד').

  דוגמה לרשומת OPT הכוללת בקשה ל- DNSSEC:

  ;; OPT PSEUDOSECTION:

  EDNS: version: 0, flags: do; udp: 4096

  <u>גודל מנה</u> *<u>דגל do</u>* *<u>גרסת EDNS</u>*

- הרחבות אחרות ממומשות ע"י שימוש במשתנים הקרויים "EDNS options". לדוגמא נבחן את הרחבת NSID. זוהי הרחבה שמטרתה לסייע בזיהוי שרת ה- DNS הספציפי שענה על השאילתה, למשל לצורך debug, כאשר יש כמה שרתים מאחורי אותה כתובת IP (מאחורי מפצל עומסים, או במימוש anycast).

  אם השרת מכבד בקשות NSID, המידע יינתן ברשומת OPT במשתנה NSID בפורמט הבא:

  מזהה ייחודי בפורמט HEX + כינוי (alias).

  לדוגמא תשובת NSID לשרת באחד ה- anycast של co.il :

  ;; OPT PSEUDOSECTION:

  ; EDNS: version: 0, flags:; udp: 4096

  ; NSID: 73 32 2e 64 65 78 ("s2.dex")

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

בעיות במימוש EDNS

ההתנהגות המצופה משרת DNS אוטוריטטיבי, המקבל שאילתה עם רשומת *OPT*, מוגדרת ב- RFC של EDNS. באופן כללי הוא אמור להתנהג באחד משני האופנים הבאים:

<u>אם הוא תומך ב-EDNS</u>: - אם התחביר (syntax) של רשומת *OPT* תקין, עליו לתת מענה כפי שהתבקש. במקרה של בעיה, עליו להחזיר שגיאה בהתאם. למשל, כאשר גרסת EDNS אינה 0 עליו להחזיר בתשובה סטטוס"*badver*".

<u>אם הוא לא תומך ב-EDNS</u>: - כלומר הוא לא יודע מה זה רשומת OPT, <u>עליו להתעלם מקיומה</u>, ולהחזיר תשובה "רגילה" כאילו השאילתה המקורית לא מכילה OPT.

בעיות ידועות:

א. **ציוד תקשורת – (FW, נתבים) בודקים בקשות DNS ומפילים אותן**

סיבות נפוצות:

- מנות UDP גדולות עלולות להחסם ע"י ציוד רשת שלא תומך בכך /לא מאפשר זאת.
- מופעים של FW אשר מופעלת בהם מדיניות בדיקת שאילתות DNS. לא אחת מתברר כי הם <u>מפילים</u> שאילתות אשר מכילות EDNS, כאשר הן אינן תואמות את המדיניות של ה- FW.
- למשל:
  - דגל EDNS שאינו מוכר ע"י ה- FW
  - גרסת EDNS לא מוכרת (שאינה 0)
  - משתנה EDNS options לא מוכר

ההתערבות של FW בשאילתות אלה <u>אינה תורמת</u> לאבטחה גדולה יותר. יש לאפשר גם שאילתות "לא סטנדרטיות" לצורך מימוש הרחבות EDNS נוספות בעתיד.

ב. **שרתים אוטוריטטיביים מיושנים/ לא מוגדרים**

- לא מספקים תשובה (time-out) ולעתים אף קורסים.
- לא מבינים מה זה option code. מחזירים סטטוסים כגון "*formerr*" או "*notimp*" עבור שאילתות תקינות.
- לא מחזירים רשומת OPT בתשובה.
- לא מחזירים סטטוס "*badver*" במקרה של גרסה לא נכונה (נצפו מקרים שחזרה תשובה עבור בקשת EDNS1, גרסה שעדיין אינה קיימת).
- וכיוצ"ב.

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

ההתנהגות המצופה משרת DNS:

התגובה לשאילתות המכילות EDNS מוגדרת היטב ב- RFC-6891. הרשימה להלן לקוחה מאתר ISC, כאן:
https://ednscomp.isc.org/compliance/summary.html

בראש הרשימה מובאת דוגמה לשאילתת EDNS "פשוטה" ותשובה תקינה. לאחריה רשימת דוגמאות של שאילתות "לא סטנדרטיות", והתגובה הנכונה לפי ה- RFC :

- **Plain EDNS**

  dig +norec +edns=0 soa zone @server

  - expect: SOA
  - expect: NOERROR
  - expect: OPT record with version set to 0
  - RFC6891

- **EDNS - Unknown Version**

  dig +norec +edns=100 +noednsneg soa zone @server

  - expect: BADVERS
  - expect: OPT record with version set to 0
  - expect: not to see SOA
  - RFC6891, 6.1.3. OPT Record TTL Field Use

- **EDNS - Unknown Option**

  dig +norec +ednsopt=100 soa zone @server

  - expect: SOA
  - expect: NOERROR
  - expect: OPT record with version set to 0
  - expect: that the option will not be present in response
  - RFC6891, 6.1.2 Wire Format

- **EDNS - Unknown Flag**

  dig +norec +ednsflags=0x80 soa zone @server

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

- expect: SOA
- expect: NOERROR
- expect: OPT record with version set to 0
- expect: Z bits to be clear in response
- RFC6891, 6.1.4 Flags

- **EDNS - DO=1 (DNSSEC)**

  dig +norec +dnssec soa zone @server

  - expect: SOA
  - expect: NOERROR
  - expect: OPT record with version set to 0
  - expect: DO flag in response if RRSIG is present in response
  - RFC3225

- **EDNS - Truncated Response**

  dig +norec +dnssec +bufsize=512 +ignore dnskey zone @server

  - expect: NOERROR
  - expect: OPT record with version set to 0
  - RFC6891, 7. Transport Considerations

- **EDNS - Unknown Version with Unknown Option**

  dig +norec +edns=100 +noednsneg +ednsopt=100 soa zone @server

  - expect: BADVERS
  - expect: OPT record with version set to 0
  - expect: not to see SOA
  - expect: that the option will not be present in response
  - RFC6891

Israel Internet Association (RA)
6 Bareket street, POB 7210
Petach Tikva 4951774
Tel: +972-3-9700900 · Fax: +972-3-9700901
info@isoc.org.il · www.isoc.org.il

איגוד האינטרנט הישראלי (ע"ר)
רחוב ברקת 6, ת.ד. 7210
פתח תקווה 4951774
טלפון: 03-9700900 · פקס: 03-9700901
info@isoc.org.il · www.isoc.org.il

מה יקרה ב-DNS Flag Day?

כאמור לעיל, יצרני ה-resolver דאגו לעקוף מקרים בהם לא מקבלת תשובה מהשרת האוטוריטטיבי. הם פיתחו מנגנונים אשר מזהים את הבעיה ומנסים להעביר לשרת האוטוריטטיבי שאילתה נוספת ללא EDNS.

זהו מצב בעייתי - משמעותו האטה בזמן התגובה לשאילתה של המשתמש. ה-resolver מחכה לתשובה, ורק אחרי ה-timeout, הוא מייצר את השאילתה הנוספת. מקרים אלה נוצרים שלא באשמת משתמש הקצה ולא באשמת ה-resolver, אלא עקב בעיות בצד האוטוריטטיבי.

ב- 1 לפברואר 2019 המעקפים על EDNS בשרתי resolver יבוטלו. כפי שהוסבר, שאילתות לשרת אוטוריטטיבי שאינו עונה לשאילתת EDNS, עלולות להיכשל.

חשוב לציין כי תרחיש זה יתקיים גם ובעיקר בכל הרזולברים הפתוחים: Quad 9: 9.9.9.9, Google: 8.8.8.8, CloudFlare: 1.1.1.1 ודומיהם.

מה יש לעשות עד 1.2.2019

ארגון ISC - Internet Systems Consortium מספק שירות שבאמצעותו ניתן לבדוק האם שם מתחם (domain) מתפרסם על שרת תקין (כלומר שהשרת האוטוריטטיבי תומך EDNS). ניתן לבדוק באתר:

https://ednscomp.isc.org/ednscomp

דף הבית של מיזם ה-DNS Flag Day מכיל גם הוא הסבר קצר ומנגנון בדיקה:

https://dnsflagday.net/

יש לוודא שהדומיין הנבדק ישרוד את השינוי, ואם לא, יש לבקש מהספק המארח לתקנו.

לשאלות והבהרות ניתן לפנות בדוא"ל ל- dnsflagday@isoc.org.il