7 ביולי 2020
ט"ו בתמוז תש"פ
סימוכין: ב-ס-1095

חולשות אשר נוצלו במרחב הסייבר בישראל במהלך השנה האחרונה

תקציר

1. מערך הסייבר הלאומי מוצא, בהתבסס על אירועים שטופלו על-ידו ומפרסומים אודות תקיפות סייבר בארץ ובעולם, כי מבין הפגיעויות העיקריות המשמשות כיום כוקטור כניסה לארגונים, בולטות פגיעויות במוצרים הבאים: שרתי SharePoint, ציוד VPN של חברת Fortine .
2. בהמשך לפעילות איתור אקטיבי של החשיפות וסיוע לגופים הרלוונטיים בצמצומם, מזהה מערך הסייבר הלאומי כי עדיין קיימים מספר רב של גופים במשק החושפים את אותן הפגיעויות, ביניהם חברות וארגונים רבים המשמשים כספקים בשרשרת אספקה של גופים חיוניים במשק.
3. מסמך זה יפרט אודות הפגיעויות ויספק המלצות להתמודדות עמן כמו גם מול הספקים המרכזיים.

רקע

4. פגיעות, חולשה או פרצת אבטחה נובעות מכשל לוגי, קידוד שגוי של תוכנה, או הגדרה שגויה, ועלולות לאפשר לתוקפים להשיג שליטה חלקית או מלאה על המחשב בו הם מותקנים, לפגוע בסודיות מידע או בזמינות שירות.
5. פגיעות בקוד עלולה להיגרם מחוסר תשומת לב של המפתח, חוסר ידע או מהימנעות מבדיקת מצבי שגיאה לא צפויים.
6. מערכת CVE (Common Vulnerabilities and Exposures) היא שיטת ייחוס לפגיעויות ידועות בתחום אבטחת מידע. חברת Mitre מתחזקת את המערכת, עם מימון של האגף להגנת הסייבר של ארה"ב.

פרטי אירוע

<u>פגיעויות במוצר SharePoint</u>

1. שרתי SharePoint משמשים לשיתוף משאבי ידע וניהולם על-ידי מספר משתמשים. ארגונים רבים משתמשים בהם על מנת להציג מידע באתרי Web פומביים.
2. בתאריך 12 בפברואר 2019 פרסמה חברת מיקרוסופט עדכון אבטחה לאחר שהתגלתה פגיעות (CVE-2019-0604) בגרסאות קודמות של המוצר, המאפשרת הרצת קוד מרחוק (RCE) על-ידי גורמים לא מורשים.
3. בחודש אפריל 2019 פרסם ה-CERT הלאומי התרעה אודות זיהוי ראשוני של ניצול הפגיעות, לאחר שהתקבלו אינדיקציות כי מתבצעים ניסיונות ניצול של החולשה לצורך התקנת WebShell בשם ChinaChopper אל מול ממשקי SharePoint החשופים לאינטרנט. בחודש דצמבר 2019 הופץ על-ידי ה-CERT הלאומי עדכון אודות זיהוי ניסיונות נוספים לניצול הפגיעות.
4. חברת אבטחת המידע פאלו-אלטו פרסמה בחודש אפריל 2019 כי זיהתה ניצול של הפגיעות על-ידי קבוצת התקיפה APT27 (AKA Emissary Panda), להתקנת Webshells בשרתי SharePoint של ארגונים ממשלתיים בשתי מדינות במזרח-התיכון. בחודש ספטמבר 2019 פרסמה החברה כי הייתה עדה לתקיפה נוספת בשיטה דומה, שוב כנגד יעדים ממשלתיים, אך לא הצליחה לשייך אותה בוודאות לאותה קבוצת תקיפה.
5. במסגרת עדכון האבטחה החודשי של מיקרוסופט (Patch Tuesday) בחודש ספטמבר 2019, פורסם כי קיימות מספר פגיעויות בשרתי SharePoint, העלולות לאפשר הרצת קוד מרחוק, בדומה לפגיעות CVE-2019-0604. בנוסף, התגלו פגיעויות העלולות לאפשר העלאת הרשאות או התחזות (Spoofing). לפירוט אודות הפגיעויות השונות ראו קישורים:
   - CVE-2019-1257
   - CVE-2019-1260
   - CVE-2019-1261
   - CVE-2019-1295

- CVE-2019-1296
- CVE-2019-1259
- CVE-2019-1262

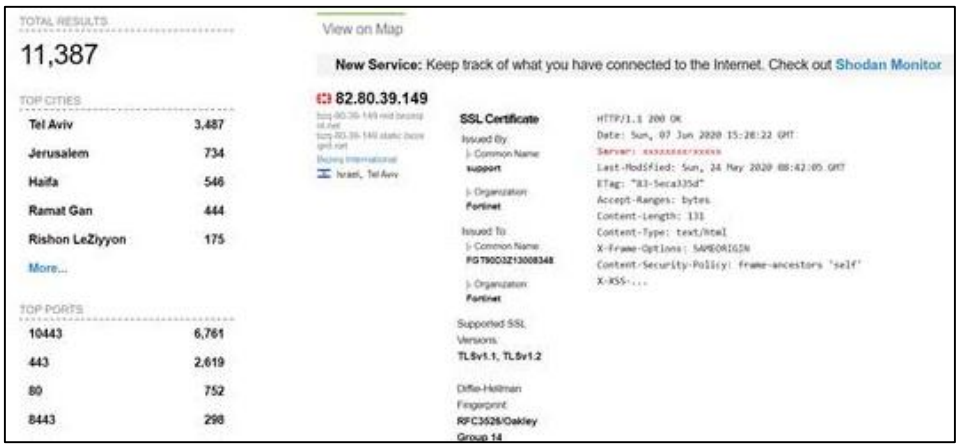
6. במסגרת עדכון האבטחה החודשי של מיקרוסופט (Patch Tuesday) בחודש מאי 2020, פורסם בי קיימות מספר פגיעויות נוספות בשרתי SharePoint, העלולות לאפשר לתוקף הרצת קוד מרחוק (RCE). לפירוט אודות הפגיעויות השונות ראו קישורים:
   - CVE-2020-1023
   - CVE-2020-1024
   - CVE-2020-1102
   - CVE-2020-1069
7. במסגרת עדכון האבטחה החודשי של מיקרוסופט (Patch Tuesday) לחודש יוני 2020, אשר פורסם ב-9 לחודש, נחשפו 12 פגיעויות נוספות במוצר. בין הפגיעות שפורסמו קיימת פגיעות קריטית העלולה לאפשר הרצת קוד מרחוק (CVE-2020-1181), וכן פגיעויות נוספות העלולות לאפשר התחזות (Spoofing), העלאת הרשאות, XSS ועוד. לפירוט אודות הפגיעויות השונות ראו קישורים:
   - CVE-2020-1289
   - CVE-2020-1148
   - CVE-2020-1183
   - CVE-2020-1318
   - CVE-2020-1295
   - CVE-2020-1298
   - CVE-2020-1323
   - CVE-2020-1297
   - CVE-2020-1178
   - CVE-2020-1177
   - CVE-2020-1320

8. סוכנות הידיעות The New Humanitarian חשפה כי בקיץ 2019 תוקפים פרצו למעל 40 שרתים של משרדי האומות המאוחדות (UN) בז'נבה ובוינה, והורידו מידע רגיש אודות הצוות, אנשים פרטיים וארגונים אשר ניהלו קשרים או קשרי מסחר עם האומות המאוחדות. התקיפה החלה בחדירה לשרת של משרד הארגון בוינה באמצעות הפגיעות CVE-2019-0604, והמשיכה בתנועה רוחבית של התוקפים ברשת הארגון עד השגת גישה למערכות משרד הארגון בז'נבה ולמשרד הנציב העליון לזכויות אדם (OHCHR) של הארגון. התקיפה התאפשרה מאחר שהארגון לא החיל את עדכון האבטחה שפורסם על-ידי מיקרוסופט, והביאה לדלף של מידע אישי, מידע בנוגע לביטוחי בריאות, מאגרי נתונים נוספים ומשאבי רשת.

<u>פגיעות בתשתית VPN של חברת Fortinet</u>

1. במהלך שנת 2019 הופצו מספר פרסומים לפיהם ציוד VPN של מספר יצרנים מובילים (Palo-Alto, Fortinet, Pulse Secure) חשוף לפגיעויות העלולות לאפשר לתוקף מרוחק ובלתי-מזוהה הרצת קוד על הציוד, או קריאה של קבצים מהציוד, כולל פרטי הזדהות של משתמשים.
2. לחלק מהפגיעויות קיים POC ברשת, וחלקן ניתנות למימוש באמצעות גישה ל-URL מסוים על ציוד ה-VPN. באוקטובר 2019 פורסם כי קיימים ברשת Exploits לפגיעויות אלו.
3. ראו התרעה שפורסמה על-ידי ה-CERT הלאומי בנושא, הכוללת פירוט אודות המוצרים הפגיעים והמלצות התמודדות.
4. נכון להיום ממשק ה – VPN הפגיע של חברת Fortinet עדיין חושף מספר רב של חברות וארגונים במשק בישראל, ומהווה שער גישה לאירועים רבים שזוהו במהלך השבועות והחודשים האחרונים.

5. מצילום המסך הבא ניתן לראות כי ציוד ה-VPN של חברת Fortinet נפוץ מאד בשימוש בישראל, ועל כן הסבירות לניצול פגיעות זו לחדירה לארגונים גבוהה.



6. חברת אבטחה המידע ClearSky חשפה כי במשך שלוש שנים נערך **קמפיין תקיפה אירני** נגד עשרות חברות וארגונים בישראל וברחבי העולם. במסגרתו, התוקפים הצליחו להשיג גישה ואחיזה ברשתות של מספר חברות וארגונים ממגזרים שונים, ביניהם IT, תקשורת, גז ונפט, תעופה, ממשלה וחברות ביטחון. על-פי הפרסום, התוקפים החלו לנצל פגיעויות בציוד VPN של Palo-Alto (CVE-2019-1579), Fortinet (CVE-2018-13379), ו-Pulse Secure (CVE-2019-11510) מספר שעות לאחר שפורסמו באופן פומבי, במטרה לחדור לרשתות של החברות הנתקפות ולשתול בהן backdoors שיובלו לנצל במועד מאוחר יותר.

דרכי התמודדות

<u>פגיעויות שונות במוצר SharePoint</u>

מומלץ לבחון ולהתקין את כלל עדכוני האבטחה לשרתי SharePoint. העדכונים האחרונים יצאו ביוני 2020.

1. הגרסאות העדכניות הן:

SharePoint Server 2019	16.0.10361.12114
SharePoint Server 2016	16.0.5017.1001

SharePoint Server 2013	15.0.5249.1001
SharePoint Server 2010	14.0.7253.5000

2. גרסאות ישנות יותר מ- SharePoint Server 2010 אינן נתמכות ומומלץ מאד לעדכנן לאחת הגרסאות הנתמכות.

<u>פגיעות בציוד VPN של חברת Fortinet</u>

1. מומלץ לבחון ולהתקין את הגרסה העדכנית ביותר של תוכנת שרת ה-Fortinet המתאימה לציוד שברשותכם.

<u>לסיכום,</u>

אנו ממליצים לכל ארגון וחברה במשק לוודא כי תשתיותיו אינן פגיעות לחשיפות אלו, כמו גם לוודא מול הספקים המרכזיים של הגוף כי גם הם הטמיעו את טלאי האבטחה. כמו כן ניתן לקיים שימוש בפתרונות הגנה קיימים לשרשרת האספקה על מנת לזהות מבעוד מועד ספקים אשר חשופים לפגיעות וחושפים את הארגון לסיכונים לעיל.

יש לציין כי גם לאחר ביצוע העדכון לא ניתן לשלול ניצול מוקדם של החשיפה והימצאותו של התוקף ברשת, ועל כן יש לבצע פעולות נוספות לזיהוי ניצול בדיעבד כפי שמפורט בהתרעת מערך הסייבר בנושא.