



## מה קורה כאשר חברה מוסמכת לדווח על חולשות אבטחה במוצריה



צפיר ליבנה

צפיר ליבנה הוא תלמיד דוקטורט בפקולטה לניהול ע"ש קולר באוניברסיטת תל אביב. תחומי המחקר שלו מתמקדים בגורמים המשפיעים על איכות המידע הציבורי ובנסיבות המביאות חברות לגלות או להסתיר מידע רלוונטי ממקבלי החלטות. מחקר הקודם של צפיר, שפורסם בכתב עת מוביל בחשבונאות יחד עם פרופ' אלי אמיר וד"ר שי לוי מהפקולטה לניהול ע"ש קולר, מצא שחברות נוטות להסתיר אירועי תקיפת סייבר מהותיים, וכאשר אלו מתגלים הם מובילים לתגובת שוק שלילית חריפה. המאמר בגיליון זה מבוסס על עבודת התזה שלו ועוסק בגילוי מידע לגבי חולשות אבטחה במוצרים.

### תקציר

בשנים האחרונות אנו עדים לגידול משמעותי בנוזקים הנגרמים מתקיפות סייבר, המביאות לשיתוק פעילותן של חברות למשך שבועות ומובילות לפגיעה תדמיתית קשה. במקרים רבים התקיפות מתאפשרות בשל חולשות אבטחה במערכות הארגון המותקף. במקביל, יצרני ציוד רפואי ומערכות רכב נאלצים לפרסם "קריאות לתיקון" (product recall) בשל גילוי חולשות קריטיות שיכולות לסכן חיי אדם. מערכת ה-CVE (Common Vulnerabilities and Exposures) של המשרד להגנת המולדת בארה"ב מהווה מקור מידע מוסמך לחולשות אבטחה, ובכך משפיעה על מקבלי החלטות בתחומי רכש וניהול סיכונים ארגוניים. מאמר זה בוחן את מידת ההשפעה שיש ליצרנים על המידע המתפרסם ברשומות ה-CVE, לאור מגמה הולכת וגוברת להעברת האחריות לרישום חולשות לארגונים המושפעים מהן. המאמר מוצא שחולשות שנרשמו על ידי היצרן זוכות לדירוג חומרה (severity) נמוך יותר בהשוואה לחולשות שנרשמו על ידי גורם בלתי תלוי. הממצאים מעלים חשש בדבר איכות המידע הציבורי לגבי חולשות אבטחה, ומדגישים את הצורך בקיום דיון ציבורי בדבר אופן ניהול המערכת בשל חשיבותה.

יודעים הרבה על מערך התמריצים הקיים לגילוי או הסתרת מידע בדבר חולשות (Silfversten et al., 2018).

## דיווח על חולשות

חוקרים באקדמיה, וכן חוקרים המועסקים על ידי חברות מסחריות, אחראים לחשיפה של חולשות אבטחה רבות (Kesan and Hayes, 2016). לדוגמה, חוקרי אבטחה מטעם חברת גוגל מצאו חולשות קריטיות במעבדים של חברת אינטל, המהווים רכיב קריטי בשיחתי הענן של גוגל. במקביל אליהם מצאו את החולשות שני צוותי מחקר שונים באקדמיה. בשני המקרים החולשות דווחו לחברת אינטל ונשמרו בחשאי מספר חודשים עד שהמידע דלף לבסוף ונודע לציבור בחודש ינואר 2018 (Jo, Silfversten et al., 2018; Silfversten et al., 2019). חברת אינטל מפעילה מנגנון המאפשר לחוקרים לדווח על חולשות, ואף מספקת תשלום לחוקרים המספקים מידע על חולשות קריטיות. במקביל לביקוש של חברות אחר מידע על חולשות במוצריהן, ניתן לראות בשנים האחרונות נידול משמעותי גם בביקוש לחולשות בלתי מוכרות (חולשות 'zero-day') בשוק האפור והשחור ולנסיקה במחיריהן של חולשות<sup>1</sup>. אם כן, ניכר שקיימים תמריצים להגברת החיפוש של חולשות. אך האם חיפוש חולשות מביא להגברת השקיפות? האם קיימים גורמים המעוניינים בהסתרת המידע?

## הסמכת חולשות

בעשרים השנים האחרונות רושם המשרד להגנת המולדת בארה"ב (U.S. Department of Homeland Security; להלן DHS) חולשות אבטחה במערכת בשם Common Vulnerabilities and Exposures (CVE). מידע על חולשות מתנקז למערכת ה-CVE ממקורות שונים, שם הוא עובר סינון ומיון ראשוני שבסופו נקבע אם המידע יפורסם ברשומות (Johnson et al., 2016; Ruohonen et al., 2018). בסוף התהליך (להלן "תהליך ההסמכה") מעריכים אנליסטים מטעם המכון הלאומי לתקנים וטכנולוגיה בארה"ב (National Institute of Standards and Technology);

בשנים האחרונות אנו עדים לנידול משמעותי בדיווחים על חולשות אבטחה במוצרים ובשירותים מבוססי תוכנה (Silfversten et al., 2018). העיסוק בסוגיות הנוגעות לפרטיות מתעצם לאור רגולציה גוברת בתחום באירופה (General Data Protection Regulation) ובארה"ב (California Consumer Privacy Act), וכן בשל תקריות שזכו לתהודה תקשורתית בחברות Facebook ו-Cambridge Analytica (2018), ו-Equifax (2017). כל אלה הביאו את העיסוק בסוגיות אבטחה לקדמת הבמה (Hedley & Jacobs, 2017). המועצה הכלכלית המייעצת לנשיא ארה"ב העריכה את הנוק לכלכלת ארה"ב מתקיפות סייבר בסכום שבין 57 ל-109 מיליארד דולר בשנת 2016 בלבד, נזקים בגובה של כ-0.5% מהתוצר המקומי הגולמי (The Council of Economic Advisers, 2018). במקרים רבים, תקיפות סייבר מתאפשרות לאור קיומן של חולשות אבטחה במוצרים ובמערכות מחשב המותקנות אצל לקוחות ארגוניים ועסקים נדולים (Arora et al., 2008; Kesan & Hayes, 2016; Sen, 2018). גורמים עוינים מנצלים פגיעויות במערכות אלו כדי להשיג נישא למידע רגיש או במטרה לחסום נישא למערכות תוך דרישת תשלום כופר.

גילוי של חולשות אבטחה יכול להביא לפגיעה תדמיתית קשה ביצרנים ובחברות המפתחות את התוכנה הפגיעה, ואף להביא לפגיעה בשווי השוק של החברה (Telang and Wattal, 2007). אי מתן גילוי על קיומן של חולשות אבטחה יכול להביא לפגיעה בלקוחות במקרים שבהם גורמים עוינים מנצלים את החולשה לצורך תקיפות סייבר (Kesan and Hayes, 2016). נוסף על כך, אי מתן גילוי הולם בדבר חולשות קריטיות יכול להיחשב כהסתרה של מידע רלוונטי מפני משקיעים, בניגוד להוראות ניירות ערך, ולהוביל לתביעות מצד משקיעים (Silfversten et al., 2018). בתמורה לדיווח על חולשות וחתירה על הסכם אי גילוי (Non-Disclosure Agreement), חברות מוכנות לשלם סכומים גבוהים לחוקרי אבטחה על מנת לצמצם את הפגיעה הפוטנציאלית בקהל לקוחותיהן (Elazari, Bar-On, 2018; Silfversten et al., 2018; Sprague & Wagner, 2018). בנוסף, ייתכן שחברות מעדיפות להחזיק במידע כדי לשלוט באופן שבו הוא יתפרסם ובתזמון הפרסום, על מנת להקטין את הפרסום השלילי בדבר חשיפת חולשות וליקויים בקוד התוכנה במוצריהן (Jo, 2019). למרות העלות הכבדה שיש לחולשות אבטחה לכלכלה העולמית, אין אנו

1 ארגוני מודיעין וממשלות זרות מוכנים לשלם סכומי עתק תמורת פרצות (exploits) בשוק האפור (Kesan and Hayes, 2016), וכן גורמים פיליים אחראים לביקושים בשוק השחור (נניש דרך רשת ה-Dark Net), הנסתר מרשת האינטרנט (Allodi, 2018). ניתן לראות מדגם מחירי פרצות בנספח א'.

## השפעת יכולת הסמכה על איכות המידע הציבורי

המאמר בוחן האם מתן הסמכה לחברה לדווח על חולשות במוצריה שלה מביא לפניעה באיכות הגילוי. המאמר מוצא שרמת החומרה של חולשות במוצרי חברות מסמיכות נמוכה בצורה משמעותית מהרמה ששררה בטרם מינוי. ההפרש בולט בעיקר כאשר משווים חולשות בהסמכה עצמית (על ידי היצרן) לחולשות שהוסמכו על ידי גורם חיצוני, באותו פרק זמן. ממצא זה מצביע על האפשרות שארגונים מנצלים את יכולת ההסמכה לרישום עצמי על מנת להשפיע על דעת הקהל בנוגע למוצריהם, באמצעות דחיית פרסום של מידע שלילי על מוצריהם ואף הסתרתו.

למעשה, המאמר עוסק ברגולציה של מידע על חולשות אבטחה. לא קיים דיון ציבורי רציני בשאלה האם כדאי להסמיך חברות לשמש כ"סוכנים אחראים" (Stewards) האמונים על גילוי מידע רלוונטי, שלם וזמין במועד. שאלה חלופית היא האם חברות מנצלות את מעמדן לבחירת מידע לגילוי באופן סלקטיבי ומוטה. הסמכת חברות לרישום חולשות במוצריהן בעצמן מהווה למעשה הקלה ברגולציה.

לצורך השוואה, קיים דיון ציבורי נרחב על המשמעויות הצפויות מהקלות רגולטוריות על מוסדות פיננסיים, כגון הקלות בדרישות לגילוי מידע. התומכים בהפחתת דרישות גילוי מידע פיננסי טוענים שחברות ידווחו לציבור על כל מידע מהותי ולא ינסו להסתיר את המידע, שכן השוק ידע להפחית את מחיר המניות שלהן לרמה שבה כבר לא ישתלם למנהלים להסתיר את המידע. גישה זו משתקפת, בין היתר, בתיאוריית החוזים הכלכלית, הנורסת שחוזי ההעסקה של מנהלים ישקפו את ההעדפות של המשקיעים לגילוי, ולפיכך מנהלים יתמרצו לגלות כל מידע רלוונטי למשקיעים גם ללא רגולציה.

המתנגדים להקלות ברגולציה טוענים שקיים כשל שוק המחייב התערבות רגולטורית כדי להגן על הציבור. זאת מכיוון שלמנהלים יש תמריץ להחזיק במידע שלילי ולא לגלותו, כל עוד משקיעים אינם יודעים שהמידע קיים. למשל, ידוע שמנהלים נוטים להסתיר תקיפות סייבר מהותיות ולתת גילוי מוקדם רק לתקיפות סייבר פחות מהותיות (Amir et al., 2018). עוד נמצא שלמנהלים יש תמריץ שלילי לתקן ליקויי אבטחה במוצרים בהיעדר רגולציה, שכן החברות נושאות בעלות התיקון המלאה אך אינן נהנות מהתועלת החברתית (Arora et al.,

להלן NIST את פוטנציאל הסיכון הטמון בכל חולשה וקובעים מדד חומרה מספרי לפי תקן Common Vulnerability Scoring System (CVSS) (Ruohonen et al., 2018).

לאור גידול משמעותי במספר החולשות, החל פרויקט ה-CVE לאפשר לחברות ולארגונים במנר הפרטי לרשום חולשות במערכת באופן עצמאי. ארגונים אלו נקראים CVE Numbering Authorities (CNA). ראשונות לקבל מינוי להסמכת חולשות היו Red Hat (בשנת 2003), חברה המפתחת מערכת הפעלה בקוד פתוח מסוג לינוקס, וכן מיקרוסופט (בשנת 2005), יצרנית מערכת ההפעלה Windows<sup>2</sup>. רישום חולשות באופן עצמאי משמעו שה-DHS מייפה את כוחם של ארגונים לשלוט במקור מידע קריטי לגבי חולשות במוצרים שלהם עצמם.

העברת האחריות מעלה תהיות בנוגע לאיכות המידע הציבורי הקיים לגבי חולשות אבטחה במוצרים ובשירותים. מצד אחד, היצרנים מכירים טוב יותר את קוד התוכנה שלהם, ולכן יכולים להכריע במהרה האם תקלה שדווחה להם מהווה חולשת אבטחה או לא. הטענה היא שכך מידע לגבי חולשות מניע במהירות רבה יותר לצרכנים, ולכן מפחית את הסיכון לניצול החולשות על ידי גורמים עוינים (Jo, 2017). טיעון זה מקבל משנה תוקף לאור ביקורת ציבורית שהופנתה כלפי פרויקט ה-CVE (MITRE-ו) (פרט) בדבר עיכובים בתהליך ההסמכה ופרסום רשומות CVE (Ruohonen et al., 2018). מצד שני, עולה כאן בעיית הנציג (Agency problem), שכן למנהלים יש תמריץ להסתיר מידע בנוגע לחולשות מהותיות במוצרים, מאחר שקבלת החלטות מצויה בידי הארגון שעליו הם אמונים ועל סמך ביצועי הם נשפטים (Silfversten et al., 2018). בהיעדר פיקוח ובקרה נאותים, ייתכן שארגונים יפרסמו מידע חלקי בלבד לגבי חולשות ויעכבו פרסום של מידע רלוונטי עבור מקבלי החלטות (Kuerbis and Badiei, 2018; Ruohonen et al., 2017)<sup>3</sup>.

2 על מנת לאתר את מועדי המינוי, בוצעה השוואה של היסטוריית השינויים באתר CVE (cve.mitre.org) דרך ארכיון האינטרנט (archive.org). בנוסף, נבדק התאריך הראשון שבו הסמיכה כל חברה חולשה בפעם הראשונה במאגר הנתונים.

3 מראיון שנערך עם חבר דירקטוריון בפרויקט ה-CVE (מייצג עמותה מקצועית של קוד-פתוח), עולה שהחשש העיקרי הוא שארגון בעל יכולת הסמכה (CNA) יסרב לרשום חולשה במוצרו, או ימנע מלפרסם רשומות CVE הנוגעות למוצרו לאורך זמן רב.

האם היעדר דיווח (על חולשות) משמעו שאין חולשות, או שהחברה מסתירה חולשות מהציבור. בשל חוסר הוודאות, יוכלו המנהלים להסתיר מידע שלילי ביתר קלות. בדומה, חברות יוכלו לפרסם מידע חלקי בנוגע לחולשות, או לתת גילוי לחולשה תוך ניסיון להמעיט בחומררתה.

## תיאור המסגרת ושיטת המחקר

חולשות אבטחה בקוד תוכנה אינן נובעות בהכרח מתקלה, מחוסר אחריות או מחוסר תשומת לב של המפתחים. אפילו הארגונים הגדולים ביותר, המחזיקים מערך בדיקות תוכנה ומתודות פיתוח המדגישות את החשיבות באבטחה ובפרטיות, מגלים בדיעבד חולשות במוצרים שפותחו, לאחר שהמוצר משווק ומותקן אצל לקוחותיהם. למרות מאמצייהן של חברות לאתר חולשות אבטחה במוצריהן, בחלק גדול מהמקרים גורמים חיצוניים הם שמדווחים על מציאת חולשות. מכיוון שכך, לארגונים ישנו קושי מובנה בשליטה ובקרה על מידע הנוגע לחולשות אבטחה במוצריהם, ומנהלים מקדישים זמן יקר לניהול משברים שנכפו עליהם בשל גילוי חולשה במוצריהם על ידי גורמים חיצוניים.

ההתבססות על תוכנה ברכיבי חומרה קריטיים מצריכה יצרנים לעמוד בדרישות אבטחת מידע נוקשות, נוסף על דרישות הבטחת איכות קיימות. לראייה, מספר חברות נאלצו לבצע קריאה לתיקון (Product recall) לאחר שביור רגולטורי קבע שקיימת סכנה מתקיפת סייבר של המוצר. דוגמה בולטת היא קריאה לתיקון של Fiat Chrysler Jeep בשנת 2015, לאחר שחוקרי אבטחת מידע פרסמו וידאו שבו תיעדו כיצד השתלטו מרחוק על הרכב שבו נסעו וגרמו לו לסטות לצד הכביש ולהידרדר לתעלה (Kessler, 2015; ICS-CERT, 2015). דוגמאות בולטות נוספות מתחום הציוד הרפואי הן קריאה לתיקון של קוצב לב מתוצרת St. Jude Medical (נרכשה על ידי Abbott Laboratories) שבו נתגלתה חולשה שיכולה לאפשר לתוקף לרוקן את הסוללה של קוצב הלב (FDA, 2017), וכן קריאה "בהולה" לתיקון של קוצב הלב (Class I) של משאבות אינסולין מתוצרת Medtronic לאחר שנתגלה כי תוקף יכול לשבש את מינון האינסולין של חולי סכרת (FDA, 2018).<sup>4</sup> קיומן של חולשות תוכנה ברכיבי חומרה קריטיים מחייב את

4 לפי הפרסום: "ה-FDA סיווג את הקריאה לתיקון כ-Class I, הרמה החמורה ביותר. שימוש במכשירים אלו יכול להוביל לפגיעה חמורה ואף למות".

בהתאם, חולשות שאינן פומביות (או חולשות ללא הקצאת מספר CVE) הן חמורות יותר (בממוצע) מחולשות פומביות (Katos et al., 2019). לפיכך, סביר להניח שקיימת הסתרה של חולשות מהותיות מהציבור, בדומה להסתרת אירועי תקיפות סייבר. אם כן, הפחתת לחץ רגולטורי למתן גילוי מידע לגבי חולשות אבטחה, מעלה את הסיכון להסתרת מידע שלילי מהותי מהציבור.

## תיאוריה והשערות מחקר

ההשערה המרכזית היא שרמת החומרה הממוצעת (Average severity) של חולשות אבטחה אצל ארגונים בעלי הסמכה לרישום עצמי תהיה נמוכה יותר מאשר זו של ארגונים ללא הסמכה כאמור. השערת המחקר נסמכת על מודל הגילוי בתנאי אי ודאות של Dye (1985). תיאוריית הגילוי הקלאסית גורסת שמנהלים המקבלים מידע פרטי שעשוי לעזור בחיזוי מצבה הכלכלי של החברה לא יוכלו להסתיר את המידע, שכן משקיעים יגיבו להסתרה בהפחתת ערך מניית החברה, עד לרמה שבה מנהלים יעדיפו לגלות את כל המידע הפרטי שבידם (מצב של "גילוי מלא" Full Disclosure) (Grossman, 1981; Milgrom, 1981). לעומת זאת, Dye מראה כי במצבים שבהם משקיעים אינם בטוחים אם מנהלים מחזיקים במידע פרטי, המנהלים יכולים להסתיר מידע פרטי בקלות רבה יותר ולחשוף רק חלק מהמידע – את המידע הפחות מזיק לשווי המניה ("גילוי חלקי"). ההסבר לגילוי החלקי הוא שמשקיעים אינם בטוחים האם מנהלים מחזיקים במידע פרטי שלילי, או שמא אינם מחזיקים במידע כלל, וחוסר הוודאות הזה מאפשר למנהלים להימנע מגילוי של מידע שלילי מאוד (Dye, 1985). לאור זאת, ניתן לצפות שבארגונים בעלי יכולת הסמכה עצמית של חולשות, תהיה למנהלים יכולת טובה יותר להסתיר מידע לגבי חולשות קריטיות לאורך זמן רב יותר. התוצאה הצפויה היא ירידה במדד החומרה הממוצע של חולשות במוצריהם של ארגונים מסמיכים, בהשוואה למצב שבו הארגון לא היה בעל יכולת הסמכה.

במסגרת המתוארת במאמר, קיימת אי ודאות אצל משקיעים ואצל ציבור הלקוחות לגבי קיומן של מידע שלילי בקשר לחולשות אבטחה. מצב זה נוצר לאור העובדה שחוקרי אבטחה וצדדים שלישיים לחברה מדווחים לה על חולשות אבטחה. מכיוון שאין דרישות גילוי, אף אחד מהמעורבים אינו מחויב לפרסם את המידע לציבור. משקיעים ולקוחות החברה אינם יודעים

היצרנים לנהל בקרת איכות לגבי אבטחת המוצר בטרם ישווק, אך גם להיערך לאפשרות שגורמים חיצוניים יאתרו חולשות ולקיים מנגנון יעיל לדיווח חולשות בדיסקרטיות.

## שיטת המחקר וממצאים

המאמר בוחן כיצד הסמכת חברות לרשום חולשות בעצמן משפיעה על רמת החומרה של חולשות מדווחות. לצורך כך, הניתוח במאמר משווה ממוצעים של מדד חומרה סטנדרטי (CVSS) בכל תקופה, ובודק אם ישנה ירידה ברמה הממוצעת בין התקופה שקודמת להסמכה לבין זו שאחריה<sup>5</sup>. מידע על חולשות ועל נתוני CVSS נלקח ממסד הנתונים National Vulnerabilities Database (NVD).

### מקרה בוחן: השוואה בין Huawei ל-Cisco

מקרה הבוחן עוסק בחברת Huawei Technologies, תאגיד סיני בענף ציוד התקשורת. שמה של Huawei נקשר במספר פרשיות ריגול עסקי וגניבת סודות מסחר לאורך השנים (Liao, 2018). בשנת 2012 זיהו סוכנויות המודיעין האמריקאיות את Huawei (יחד עם חברת ZTE הסינית) כגורם המאיים על הביטחון הלאומי של ארה"ב (Sanger and Perlroth, 2014). המודיעין האמריקאי חושש שהממשל הסיני יורה לחברת Huawei להשאיר דרכי גישה בדמות "דלתות אחוריות" (backdoors) לציוד שהחברה מוכרת, וכך יוכל המודיעין הסיני לרגל אחר מטרות אמריקאיות בחופשיות. בעקבות מציאת סדרה של חולשות אבטחה במוצרי החברה, החליט הממשל לאסור על כל הגופים הפדרליים לבצע רכש או לקנות שירותים מהחברה (Woo, 2019).

בסוף שנת 2016 הוסמכה Huawei לרשום חולשות בעצמה. איור מס' 1 מציג השוואה בין כמות החולשות שפורסמו במוצרי החברה, לבין כמות החולשות שפורסמו במוצרי חברת Cisco Systems. היא המתחרה העיקרית של Huawei בתחום ציוד התקשורת (התחום העיקרי שבו פועלות שתי החברות). כמו כן, נערכת השוואה בין רמת החומרה הממוצעת של חולשות במוצרי שתי החברות בכל תקופה. חברת Cisco

הוסמכה לרשום חולשות במוצריה כבר בשנת 2007, ולכן נתונה משמשים כקבוצת ביקורת (control group) לנתוני Huawei.

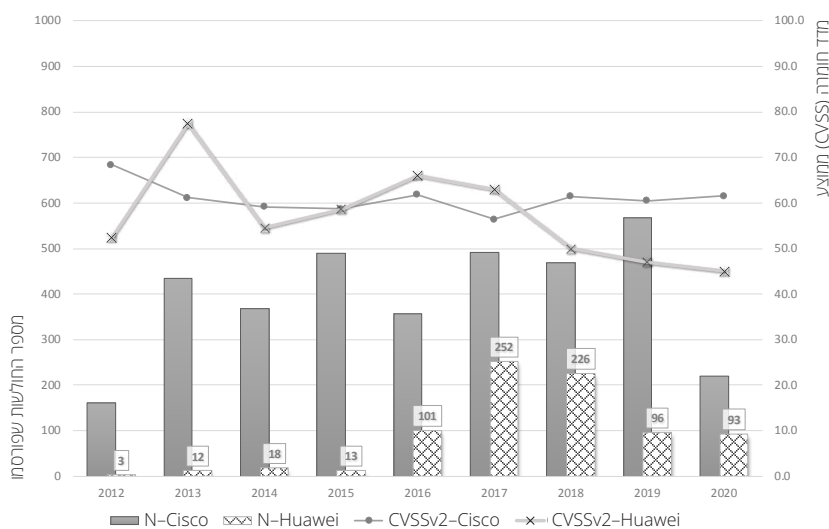
**איור 1:** חולשות במוצרי החברות Huawei Technologies ו-Cisco Systems, לכל שנה בין השנים 2012 ועד 2020. כמות החולשות שפורסמו ב-NVD במוצריה של כל חברה מוצג בעמודות (בחלקו התחתון של הגרף). רמת החומרה הממוצעת של כל חברה מוצגת בגרף המגמה (בחלקו האמצעי-עליון של הגרף). רמת החומרה היא מדד ה-CVSS הממוצע של כלל החולשות שפורסמו בכל שנה במוצריה של כל אחת משתי החברות.

לאחר הסמכתה לרשום חולשות במוצריה, ירדה רמת החומרה הממוצעת של חולשות במוצרי Huawei ב-32% (מרמה של 66.0 בשנת 2016 לרמה של 45.0 בשנת 2020). באותה התקופה כמעט שלא חל שינוי ברמת החומרה הממוצעת של חולשות במוצרי Cisco (מרמה של 61.8 בשנת 2016 ועד רמה של 61.6 בשנת 2020). מנגד, ניתן לטעון ש-Huawei למעשה פעלה להגדלת כמות החולשות שהביאה לפרסום (על ידי הסמכתן) ובכך הגבירה את רמת השקיפות של דיווחיה. טענה זו מקבלת צידוק מסוים בכך שכמות החולשות הקריטיות עלה מ-21 בשנת 2016 ל-38 בשנה העוקבת. אך עלייה זו לא נמשכה, שכן בשנת 2018 צנח מספר החולשות הקריטיות של Huawei ל-11, ובשנת 2019 מספר החולשות עמד על חמש בלבד. גם שיעור החולשות הקריטיות מתוך סך החולשות במוצריה צנח מ-21% ב-2016 (בטרם המינוי) עד ל-5% בשנת 2019. באותה התקופה חל גידול מתמיד במספר החולשות הקריטיות במוצרי חברת Cisco, מ-36 בשנת 2016 (10% מסך החולשות) ועד ל-78 בשנת 2019 (14% מסך החולשות). איור מס' 2 מציג את השינוי במנמת החומרה של חולשות במוצרי Huawei לעומת מוצרי Cisco בחתך רבעוני.

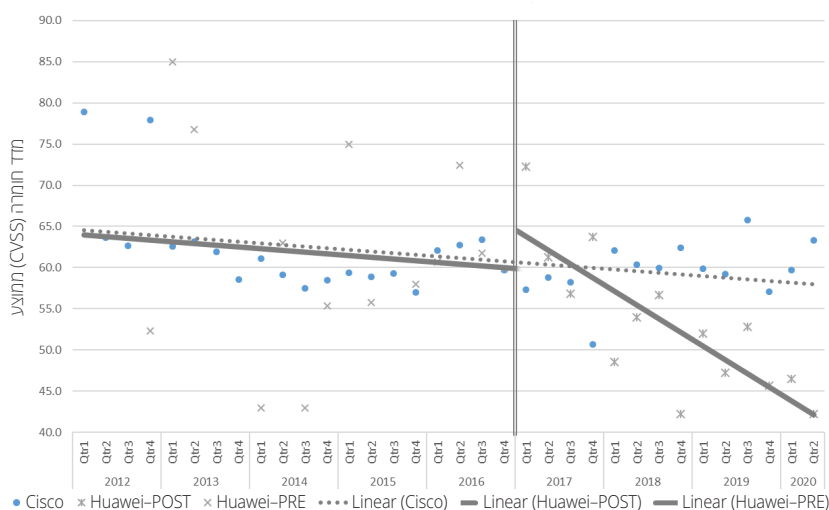
**איור 2:** השוואה של מדד CVSS רבעוני ממוצע של חברת Huawei (קו רציף) לעומת זה של חברת Cisco (קו מקווקו). הקו האנכי מציין את מועד תחילת ההסמכה העצמית של Huawei. מדד ה-CVSS מציין את רמת החומרה (severity) של חולשות במוצרי החברה, כפי שנקבע על ידי אנליסטים של NIST במשרד המסחר האמריקאי.

5 נתוני ה-CVSS מצויים במערכת ה-NVD וזמינים להורדה דרך האתר <https://nvd.nist.gov>

איור 1: מקרה בוחן; כמות חולשות ומדד חומרה ממוצע



איור 2: מקרה בוחן; הבדלים במגמות פרסום חולשות סביב מינוי Huawei כארגון מסמך



זאת "הסמכה עצמית". הניתוח מבוסס על שיטת הפרשי הממוצעים בין קבוצות שונות (Difference-in-Differences, DiD), תוך שימוש ברגרסיה ליניארית. מכיוון שארגונים שונים קיבלו את יכולת ההסמכה מה-DHS בזמנים שונים, מדובר למעשה בניתוח "אימוץ מדורג" (Staggered Adoption). בשיטה זו משווים בין רמת ה-CVSS הממוצעת של יצרנים שהחלו הסמכה עצמית של חולשות לבין הרמה הממוצעת ששררה בטרם מונו כמסמיכים. כקבוצת ביקורת בוחנים את רמת ה-CVSS הממוצעת בקרב ארגונים שטרם החלו להסמיך (או בקרב ארגונים שלא רכשו יכולת הסמכה כלל לאורך תקופת המדגם).

## ניתוח סטטיסטי

בעוד מקרה הבוחן מצביע על יתרון עבור חברות השולטות על מידע הנוגע לחולשות במוצריהן, יש צורך להרחיב את הדיון לארגונים נוספים, וכן לראות אם התופעה קיימת גם לאורך זמן ובקרב ארגונים נוספים. לפיכך, המאמר פונה כעת לניתוח סטטיסטי על מדגם רחב הכולל 31 ארגונים, לאורך 22 שנים, הנוגע ל-52,438 חולשות ובסך הכול 61,621 תצפיות (כל חולשה משייכת למוצרי ארגון אחד או מספר ארגונים, ולכן מספר התצפיות גדול ממספר החולשות). כאשר יצרן מקבל יכולת הסמכה ורושם חולשות במוצריו, ניתן לכנות

בטבלה 1 מוצגים ממצאים מניתוח השפעת יכולת ההסמכה של ארגונים (CNA) על רמת החומרה של חולשות (מדד CVSS). השערת המחקר גורסת שארגונים ינצלו את מעמדם כגורם מסמך על מנת להפחית את רמת החומרה של חולשות במוצריהם. ההשערה נבחנת על ידי שימוש ברגרסיה הבאה:

$$\log(CVSS_v) = CNA_i + Adopted_{ti} + SelfAssigned_{vi} + FE_t + FE_i + \varepsilon_v$$

כאשר המשתנה התלוי הוא פונקציית לוג של מדד החומרה (CVSS). הסימון  $v$  מייצג חולשה (לכל חולשה מזהה ייחודי CVE-ID), כאשר לכל חולשה ישנו גורם מסמך וכן זמן שבו החולשה מתפרסמת  $t$ . כל חולשה יכולה להיות במוצרי ארגון יחיד או במספר ארגונים, כל אחד מהם מסומן באות  $i$ .

המשתנים המסבירים הם מסוג בינארי (מקבלים ערכים 1 או 0). ארגון בעל יכולת הסמכה מסווג כ-1 CNA לכל אורך המדגם (treatment group). בעמודה מס' 1 בטבלה ניתן לראות, למשל, שחולשות במוצרי ארגונים מסמיכים מסווגות עם מדד חומרה (CVSS) גבוה ב-3.2% מאשר חולשות במוצרי ארגונים שאינם מסמיכים. ההפרש הזה הוא ממוצע משוקלל של הפרשים הנמדדים בכל יחידת זמן (רבעון קלנדר) כדי לנטרל השפעות הקשורות לממד הזמן (שינויים טכנולוגיים, הבדלי מדידה וסיווג, שינויים במידת הסיכון של חולשות). לאחר מינוי ארגון כמסמך, חולשות במוצרי יסווגו  $Adopted=1$ . חולשות במוצרי ארגונים יסווגו עם  $CNA=1$  וכן  $Adopted=0$  בכל מקום שבו פורסמו חולשות במוצריהם במועד שקדם למינויים. בעמודה מס' 2 ניתן לראות שחולשות במוצרי ארגונים שהפכו למסמיכים הן בעלות דירוג CVSS גבוה יותר ב-5.1% (בממוצע) בהשוואה לחולשות במוצרי ארגונים שטרם מונו כמסמיכים באותה תקופת זמן. לכאורה מדובר בממצא המנוגד להשערת המחקר – חולשות במוצרי ארגונים שקיבלו לידיהם יכולת הסמכה זוכות לסיווג חומרה גבוה יותר מאשר חולשות במוצרי ארגונים שאינם בעלי יכולת הסמכה. אם ארגונים אלו מנסים להביא להפחתה ברמת החומרה, נראה כי הם נכשלים במשימתם. עם זאת, הסבר חלופי יכול להימצא ברמת סיכון גבוהה יותר לקבוצה זו.

כדי לבחון כיצד משפיעה יכולת ההסמכה על רמת החומרה של חולשות, נעשה שימוש במשתנה שלישי לסיווג הגורם המסמך את החולשות. כאשר ארגונים מסמיכים את החולשות במוצריהם בעצמם ("הסמכה עצמית") אזי הרשומה מסווגת כ-1 SelfAssigned. משתנה זה מאפשר להבדיל בין היכולת להסמך חולשות לבין ההסמכה בפועל. בעמודה מס' 3 בטבלה

ניתן לראות שרמת החומרה של חולשות הנוגעות למוצרי ארגונים בעלי יכולת הסמכה גבוהה ב-11% מזו של חולשות הנוגעות למוצרי ארגונים שאינם בעלי יכולת כזו על פני אותה תקופת זמן. עם זאת, במקרים שבהם חולשות הוסמכו עצמאית (self-assigned), רמת החומרה יורדת ב-8.5%. יחדיו, ממצאים אלה מתאימים להסבר שלפיו ארגונים מסמיכים הם בעלי "פרופיל סיכון" גבוה יותר, המתבטא ברמת חומרה ממוצעת גבוהה יותר, אולם הגישה האקטיבית (הסמכה בפועל של החולשות במוצריהם) מאפשרת הפחתה משמעותית ברמת החומרה (הפחתה של יותר מ-8%).

כאשר הניתוח מתבצע ברמת הארגון הבודד (within-vendor), נמצא שארגונים שקיבלו לידיהם את יכולת ההסמכה רואים ירידה של 6.4% ברמת החומרה הממוצעת של חולשות בהשוואה לרמה ששררה בארגון טרם המינוי (עמודה מס' 4). בניתוח נוסף (עמודה מס' 5) נמצא שרמת החומרה הממוצעת של ארגונים מסמיכים למעשה גבוהה יותר ב-4.7% בהשוואה לתקופה שקדמה למועד ההסמכה, דבר המעיד על עלייה ברמת הסיכון. עם זאת, הירידה המתוארת בעמודה מס' 4 מקורה ביכולת ההסמכה העצמית של ארגונים – רמת החומרה של חולשות נמוכה יותר ב-14% כאשר ארגון מסמך את החולשות בעצמו, לעומת מצב שבו גורם חיצוני מסמך חולשות במוצריו. הממצאים דומים גם כאשר האפקט נמדד במקביל בארגונים שונים החווים אותו באותה תקופת זמן (Within-vendor, within period). כך, בעמודה 6 ניתן לראות כי האפקט של המינוי חלש יותר (אפקט שלילי מובהק של 3.1% לעומת 6.4% במקרה של ניתוח Within-vendor). זוהי בוודאי תוצאה של הפרש הנמדד על פני תקופת זמן קצרה (רבעון), כך שישנן פחות תצפיות להשוואה. עם זאת, היתרון במדידת האפקט בתקופת זמן קצרה הוא הפחתת החשש שישנם אירועים חיצוניים נוספים שלא נלקחו בחשבון (confounding events) והשפיעו על התוצאה. תוצאה דומה קיימת גם בעמודה מס' 7, המתארת הפרש של 6.3% ברמת החומרה של חולשות במוצרי ארגון שמונה כמסמך, עבור חולשות שארגונים חיצוניים הסמיכו לאחר מועד המינוי, לעומת התקופה שקדמה למועד המינוי (וממש בסמוך לו). עוד ניתן לראות כי במצב זה חולשות בהסמכה עצמית הן בעלות רמת חומרה נמוכה ב-12.6% לעומת חולשות בהסמכה חיצונית, בהשוואה לארגונים אחרים באותה תקופת זמן. ממצאים אלו תומכים בהשערת המחקר, שכן ארגונים בעלי יכולת הסמכה הנמצלים את כוחם כדי להסמך חולשות במוצריהם, מביאים לירידה במדד ה-CVSS לאחר קבלת היכולת להסמך.

טבלה 1: השפעת יכולת ההסמכה על רמת מדד החומרה של חולשות

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
VARIABLES	log_CVSS	log_CVSS	log_CVSS	log_CVSS	log_CVSS	log_CVSS	log_CVSS
isCNA	0.032*** (7.779)	-0.004 (-0.669)	-0.003 (-0.397)				
isAdopted		0.051*** (8.063)	0.110*** (15.761)	-0.064*** (-12.363)	0.047*** (6.660)	-0.031*** (-4.316)	<b>0.063***</b> <b>(7.612)</b>
isSelfAssigned			-0.085*** (-19.782)		-0.140*** (-25.590)		<b>-0.126***</b> <b>(-23.324)</b>
Vendor Group FE	-	-	-	Yes	Yes	Yes	Yes
Assignment Year, Publishing Quarter FE	Yes	Yes	Yes	-	-	Yes	Yes
Observations	61,621	61,621	61,621	61,635	61,635	61,621	61,621
F Statistic	60.5	70.7	187.8	152.8	427.4	18.6	280.2
Adj. R <sup>2</sup>	0.048	0.049	0.054	0.105	0.117	0.142	0.151
Adj. R <sup>2</sup> within	0.001	0.002	0.008	0.003	0.015	0.000	0.011

Robust t-statistics in parentheses. All regressions are clustered by CVE-ID (unique vulnerability identifier).

\*\*\* p<0.01, \*\* p<0.05, \* p<0.1

ב-16.9%, אם החולשה בהסמכה עצמית (לעומת הסמכה המבוצעת בסמוך לאותו מועד על ידי גורם חיצוני).

## סיכום ומסקנות

בדוגמה המוצגת במאמר, Huawei, בדומה ל-Cisco, השיגה שליטה על פרסום החולשות במוצריה, וכך הביאה לירידה במדד ה-CVSS הממוצע. מאז מועד הסמכתן, שתי החברות אחראיות לרישום של קרוב ל-100% מהחולשות במוצריהן, כך שניתן לשער שהחברות שולטות ביד רמה במידע המתפרסם בנוגע למוצריהן. התמודדותה של Huawei עם גילויים חיצוניים במהלך השנים האחרונות (וביתר שאת מאז 2018) בדבר חולשות אבטחה מהותיות במוצריה, חיידה את הבעייתיות

נוסף על הבחינה של השינוי ברמת החומרה הממוצעת, נבחן גם אם ישנו שינוי בהסתברות שחולשה תסווג כ"קריטית" (רמת 90-100 CVSS) לאור יכולת ההסמכה של ארגונים. דיווחים בתקשורת בדרך כלל נסובים סביב חולשות "קריטיות" והשפעתן הפוטנציאלית על עסקים המשתמשים בתוכנה (ופחות סביב חולשות ברמות חומרה נמוכה יותר). לאור זאת, במקרה שהחולשה בעלת דירוג "קריטי" (90 ומעלה), הבדיקה נעשית בשנית תוך שימוש במשתנה תלוי בינארי השווה ל-1. הממצאים מתוארים בטבלה 2 ועומדים בקנה אחד עם הממצאים המתוארים לעיל, כאשר ההסתברות שחולשה תסווג כ"קריטית" יורד ב-4.1% לאחר שארגון מקבל מינוי כמסמיך (עמודה מס' 4). כמו כן, היכולת להסמיך מאפשרת לארגונים להפחית את הסיכון שחולשה תסווג כ"קריטית"



טבלה 2: השפעת יכולת ההסמכה על ההסתברות לסיווג חולשה לרמת חומרה קריטית

	(1)	(2)	(3)	(4)	(5)	(6)	(7)
VARIABLES	isCritical	isCritical	isCritical	isCritical	isCritical	isCritical	isCritical
isCNA	0.056*** (16.639)	0.020*** (3.527)	0.022*** (3.890)				
isAdopted		0.049*** (8.338)	0.116*** (16.921)	-0.041*** (-7.649)	0.107*** (14.008)	-0.025*** (-3.590)	<b>0.102*** (12.227)</b>
isSelfAssigned			-0.096*** (-21.509)		-0.187*** (-30.118)		<b>-0.169*** (-28.195)</b>
Vendor Group FE	-	-	-	Yes	Yes	Yes	Yes
Assignment Year, Publishing Quarter FE	Yes	Yes	Yes	-	-	Yes	Yes
Observations	61,631	61,631	61,631	61,645	61,645	61,631	61,631
F Statistic	276.8	190.8	306.8	58.5	518.5	12.9	406.3
Adj. R <sup>2</sup>	0.074	0.075	0.083	0.136	0.156	0.191	0.207
Adj. R <sup>2</sup> within	0.003	0.004	0.012	0.001	0.025	0.000	0.020

Robust t-statistics in parentheses. All regressions are clustered by CVE-ID (unique vulnerability identifier).

\*\*\* p<0.01, \*\* p<0.05, \* p<0.1

למוצריהן. בכך, יכולים ארגונים מסמיכים להפחית את הסיכון לנזק תדמיתי כתוצאה מגילוי חולשות במוצריהם.

מחקר נוסף נדרש על מנת לבסס את הקשר הסיבתי שבין יכולת ההסמכה לבין השינוי ברמת החומרה של חולשות. המאמר מציב זרקור על נושא שלא זכה לניתוח אקדמי משמעותי, וכן חומק מעיניהם של קובעי מדיניות ורגולטורים המנסים למצוא פתרונות שיסייעו למגר סיכונים אבטחה ופרטיות. נוסף על כך, תחום זה מגלם בתוכו עולם תוכן עשיר שיכול להוות כר פורה למחקרים אמפיריים עתידיים הנוגעים לגילוי או להסתרה של מידע מהותי.

tsafir@livne@mail.tau.ac.il

צפריר ליבנה

במתן שליטה על גילוי חולשות לחברות כמותה. הממצאים מחזקים את ההשערה שחברות שהוסמכו לרשום חולשות במוצריהן מנצלות את מעמדן לצורך ניהול אקטיבי של תדמיתן, כפי שזו מצטיירת מרמת האבטחה של מוצריהן.

בדומה למסקנות העולות ממקרה הבוחן, ניתן להסיק מסקנה דומה לאור ממצאי הניתוח הסטטיסטי על המדגם הרחב יותר. ארגונים בעלי יכולת הסמכה הם בעלי "פרופיל סיכון גבוה יותר", כאשר חולשות במוצריהם נוטות להיות בעלות דירוג חומרה גבוה יותר. עם זאת, חולשות בהסמכה עצמית הן בעלות דירוג חומרה נמוך יותר באופן משמעותי, וכן הסבירות שחולשה בהסמכה עצמית תסווג כ"קריטית" היא נמוכה באופן משמעותי. לאור זאת, ניתן לומר שיכולת ההסמכה העצמית מאפשרת לארגונים לשלוט במידע המפורסם הנוגע

- Allodi, L. (2018). Underground Economics for Vulnerability Risk, *login.*, 43(1), 6-10.
- Amir, E., Levi, S. and Livne, T., (2018). Do Firms Underreport Information on Cyber-Aattacks? Evidence from Capital Markets, *Review of Accounting Studies*. 23(3), 1177–1206.
- Arora, A., Telang, R. and Xu, H. (2008). Optimal Policy for Software Vulnerability Disclosure, *Management Science*. 54(4), 642–656.
- Dye, R.A. (1985). Disclosure of Nonproprietary Information, *Journal of Accounting Research*, 23(1), 123-145.
- Elazari Bar-On, A. (2018). Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties, in Ellis, R. and Mohan, V. (eds) *Rewired: Cybersecurity Governance*. Wiley, p. 42.
- FDA (2017). Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers, *FDA Safety Communication*.
- FDA (2018). Medtronic Recalls Remote Controllers for MiniMed Insulin Pumps for Potential Cybersecurity Risks, Class I Recall. *FDA Safety Communication*.
- Grossman, S.J., (1981). The Informational Role of Warranties and Private Disclosure about Product Quality, *The Journal of Law & Economics*, 24(3), 461–483.
- Hedley, D. and Jacobs, M., (2017). The Shape of Things to Come: the Equifax Breach, the GDPR and Open-Source Security, *Computer Fraud and Security*, (11), 5–7.
- ICS-CERT (2015), Harman-Kardon Uconnect Vulnerability (ICSA-15-260-01), *ICS Advisory*.
- Jo, A.M., (2017). The Effect of Competition Intensity on Software Security – An Empirical Analysis of Security Patch Release on the Web Browser Market.
- Jo, A.M., (2019). Software Vlnerability Disclosure and Security Investment, *Workshop on the Economics of Information Security (WEIS 2019)*.
- Johnson, P., Gorton, D., Lagerström R., and Ekstedt, M., (2016). Time Between Vulnerability Disclosures: A Measure of Software Product Vulnerability, *Computers & Security*, 62, 278–295.
- Katos, V., Rostami, S., Bellonias, P., Davies, N., Kleszcz, A., Faily S., Spyros, A., Papanikolaou, A., Ilioudis C., and Rantos K., (2019). *State of Vulnerabilities 2018/2019 – Analysis of Events in the life of Vulnerabilities*, ENISA – The European Union Agency for Network and Information Security.
- Kesan, J.P. and Hayes, C.M., (2016). Bugs in the Market: Creating a Legitimate, Transparent, and Vendor-Focused Market for Software Vulnerabilities, *Arizona Law Review*, 58(3), 753–830.
- Kessler, A.M., (2015). Fiat Chrysler Issues Recall Over Hacking', *The New York Times*, 24 July 24, 2015.
- Kuerbis, B. and Badiei, F., (2017). Mapping the Cybersecurity Institutional Landscape, *Digital Policy, Regulation and Governance*, 19(6), 466–492.
- Liao, S., (2018). Verizon Won't Sell Huawei Phones Due to US Government Pressure, Rreport Says', *The Verge*, January 30, 2018.

Milgrom, P.R. (1981). Rational Expectations, Information Acquisition, and Competitive Bidding, *Econometrica*. 49(4), 921–943.

Ruohonen, J., Rauti S., Hyrynsalmi S., and Leppänen V., (2018). A Case Study on Software Vulnerability Coordination, *Information and Software Technology*, 103, 239-257.

Sanger, D.E. and Perloth, N., (2014). NSA Breached Chinese Servers Seen as Security Threat, *The New York Times*, March 22, 2014.

Sen, R. (2018). Challenges to cybersecurity: Current state of affairs', *Communications of the Association for Information Systems*, 43(1),22–44.

Silfversten, E., Phillips, W.D., Paoli, G.P., and Ciobanu, C., (2018), *Economics of Vulnerability Disclosure*,

ENISA- The European Union Agency for Network and Information Security, doi: 10.2824/49807

Sprague, C. and Wagner, J. (2018). Economic Motivations for Software Bug Bounties, *Economics Bulletin*, 38(1), pp. 550–557.

Telang, R. and Wattal, S. (2007). An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price', *IEEE Transactions on Software Engineering*, 33(8), 544–557.

The Council of Economic Advisers (2018). *The Cost of Malicious Cyber Activity to the U.S. Economy*.

Woo, S., (2019). Huawei Equipment Has Major Security Flaws, U.K. Says, *Wall-Street Journal*, March 28, 2019.

## נספח א': עשרים הארגונים בעלי מספר החולשות הגבוה ביותר

עשרים הארגונים המובילים לפי מספר החולשות, סוג הארגון, מספר החולשות, המוצר הפגיע ביותר (לפי מספר האזכורים ברשומות), סוג המוצר, וכן מחירים שארגונים שונים מוכנים לשלם עבור חולשות קריטיות במוצרים של הארגון (מחיר מקסימלי). המחירים נלקחו מאתרי הארגונים (תוכניות תשלום לחוקרים מסוג Bug Bounty שמפעילים הארגונים בעצמם), וכן מגורם הרוכש חולשות ומוכר לצדדים שלישיים ("שווק אפור", הנתונים באדיבות חברת Zerodium).

Name of organization	Organization type	Vulnerabilities	Most vulnerable product	Type of product	Vendor price	Market price (Zerodium)
<b>Microsoft Corporation</b>	Public Company	12,515	Windows	Operating System	\$ 250,000	\$ 1,000,000
<b>Apple Inc.</b>	Public Company	7,893	Safari Web Browser	Software	\$ 1,500,000	\$ 2,000,000
<b>Oracle Corporation</b>	Public Company	6,840	MySQL Database Management System	Software (open-source)	-	-
<b>Google LLC</b> , subsidiary of <i>Alphabet Inc.</i> (2015)	Public Company	6,387	Chrome Web Browser	Software (open-source)	\$ 1,500,000	\$ 2,500,000
<b>IBM Corporation</b>	Public Company	5,105	Websphere Web Server	Software	-	-
<b>Cisco Systems, Inc.</b>	Public Company	4,527	Cisco Internetwork Operating System (IOS)	Operating System	-	\$ 10,000
<b>The Linux Foundation</b>	Non-Profit	4,132	Linux Kernel	Operating System (open-source)	-	-
<b>The Debian Project</b> , supported by <i>Software in the Public Interest, Inc.</i>	Non-Profit	4,027	Debian Linux	Operating System (open-source)	-	\$ 50,000
<b>Adobe Inc.</b>	Public Company	3,562	Flash Player	Software	-	\$ 80,000
<b>Red Hat, Inc.</b> , acquired by <i>IBM Corporation</i> (2019)	Public Company	3,436	Red Hat Enterprise Linux	Operating System (open-source)	-	\$ 50,000
<b>Canonical Ltd.</b>	Private Company	2,446	Ubuntu Linux	Operating System (open-source)	-	\$ 50,000
<b>The Mozilla Foundation</b>	Non-Profit	2,351	Firefox Web Browser	Software	-	\$ 100,000
<b>HP Inc.</b>	Public Company	1,996	HP System Management Homepage	Software	-	-
<b>Sun Microsystems Inc.</b> , acquired by <i>Oracle Corporation</i> (2010)	Public Company	1,740	Java Runtime Environment	Software	-	-
<b>openSUSE Project</b> , sponsored by <i>SUSE Linux GmbH</i>	Private Company	1,601	openSUSE Linux	Operating System (open-source)	-	-
<b>Apache Software Foundation</b>	Non-Profit	1,386	Tomcat Java Server	Software	-	\$ 500,000
<b>Fedora Project</b> , sponsored by <i>Red Hat, Inc.</i>	Public Company	1,025	Fedora Linux	Operating System (open-source)	-	\$ 50,000
<b>QUALCOMM Incorporated</b>	Public Company	899	Snapdragon LTE Modem	Hardware	-	-
<b>Joomla!</b> , supported by <i>Open Source Matters, Inc.</i>	Non-Profit	851	Joomla! Content Management System	Software (open-source)	-	\$ 10,000
<b>Huawei Technologies Co., Ltd.</b>	Private Company	819	Secospace Firewall	Operating System (firmware)	-	\$ 200,000