העדכון שלפניכם לוקט ועובד במסגרת פעילות ה-CERT הלאומי על בסיס מגוון מקורות רחב, כדי לרכז מידע רלוונטי ואקטואלי לעוסקים בתחום הגנת הסייבר. כפועל יוצא, ה-CERT הלאומי אינו יכול לערוב לחלוטין למידע המובא בעדכון או למסקנות המשתמעות ממנו, ואין באמור בעדכון משום המלצה לנקיטת פעולות כלשהן או לשינוי מדיניות אבטחה קיימת. אין באזכור חברות אבטחה או גורמים מסחריים אחרים משום הבעת עמדה או המלצה ביחס אליהם או לשירותים או המוצרים המוצעים על ידם.

17 יולי 2015

א' אב תשע"ה

סימוכין: ל-ס- 139

הנדון: חולשה במערכת Adaptive Security Appliance

לאחרונה הגיע לידי ה- CERT הלאומי מידע אודות סריקות להמצאות חולשה במערכות Adaptive Security Appliance (ASA) של חברת CISCO. מדובר ברכיב אבטחה ייעודי המספק מגוון רחב של שירותי אבטחת מידע ארגוניים מודולאריים המאפשרים הרחבה לשירותי אבטחת מידע נוספים.

החולשה נתגלתה לראשונה בשנת 2014, ואף פורסם לה טלאי אבטחה ע"י חברת CISCO. ב- CERT הלאומי התקבלו דיווחים אודות עדויות כי סריקות אלו גרמו לנפילתם של כ-100 רכיבי ASA. ככל הנראה הסריקה לא בוצעה כחלק מפעילות זדונית.

החולשה קיימת במימוש מנגנון IKE (Internet Key Exchange) שאחראי על בניית Tunnel ה- VPN בין שני צדדים. ניצול החולשה מאפשר ביצוע Denial Of Service באמצעות שליחת פקטות UDP זדוניות, CVE-2014-3383.

חברת CISCO ממליצה לכל משתמשי ASA לעדכן גרסה על מנת להימנע מתקיפות עתידיות.

קישורים ומידע נוסף ניתן למצוא באתר של חברת CISCO:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa

במידה שבבדיקתכם התגלה ממצא כלשהו נבקש לקבל היזון חוזר.
לכל מידע נוסף ניתן לפנות אלינו.

הערה: שיתוף מידע עם ה- CERT הלאומי איננו מחליף חובת דיווח לגוף מנחה כל שהוא, במידה שהתגלה צורך כזה.

בברכה,

CERT-IL

טל: 03-7450801

team@cert.gov.il

המידע המובא לעיל לוקט ועובד על ידי CERT-IL במטרה לספק ידע רלוונטי ואקטואלי לעוסקים בתחום ההגנה בסייבר לטובת השכלה וידע כללי. אין במידע זה משום המלצה לנקיטת פעולות כלשהן או לשינוי מדיניות אבטחה קיימת. אין באזכור חברות אבטחה או גורמים מסחריים אחרים משום הבעת עמדה או המלצה ביחס אליהם או לשירותים או המוצרים המוצעים על ידם.