מקור הפגיעות ברכיב קריפטוגרפי, המאפשר לתוקף • Windows 10-מיקרוסופט פרסמה אמש פירצת אבטחה חמורה ב זיוף תעודות דיגיטליות מסוג מסוים • מאחר ופוטנציאל התקיפה הוא חריג בגודלו, מומלץ לבחון ולהתקין את העדכון במערכות השונות בהקדם האפשרי

09:40 | 15.1.2020טכנולוגיה

התרעת סייבר |

עיבוד: מערך הסייבר הלאומי

מבית מיקרוסופט ופורסמה אמש בדחיפות על Windows מערך הסייבר הלאומי מתריע מפני פירצת אבטחה חמורה שהתגלתה במערכת ההפעלה 10 ידי החברה. המערך קורא לציבור הרחב ולארגונים לעדכן בהזדמנות הראשונה ובמיידיות את עדכון האבטחה ששחררה החברה.

מדי חודש בחודשו משחררת מיקרוסופט עדכוני אבטחה שוטפים המגנים על התוכנה מפני התקפות ורוגלות. פירצת האבטחה, שהעדכון שלה פורסם אמש: Windows 10, Server 2016, 2019, Server core – נחשבת חמורה במיוחד בשל היקפה החריג. הפירצה נוגעת למערכות ההפעלה הנפוצות מאוד ומותקנות על עשרות מיליוני מחשבים בעולם.

על פי מיקרוסופט, טרם נצפו תקיפות הממשות פירצה זו, אך במערך הסייבר מעריכים היום כי לא ייקח זמן רב עד שפגיעויות אלו ישמשו בפועל לתקיפות סייבר מאחר שפוטנציאל התקיפה דרכן חריג בהיקפו. המשמעות היא כי כל מחשב המריץ גרסה פגיעה של מערכת ההפעלה מסוג וינדוס 10 עלול להוות בפוטנציאל יעד לתקיפה, אם לא יעודכן בו עדכון האבטחה הנוכחי.

מערך הסייבר הלאומי קורא לציבור ולארגונים לוודא שמערכות ההפעלה שלהם מעודכנות עם העדכון האחרון. למשתמשים פרטיים, מומלץ לבצע של מערכת ההפעלה באמצעות הכלים המובנים בה ("Update Now") עדכון יזום.

המשמש לטיפול, בדיקה ואישור של תעודות דיגיטליות ומסרים, dll.crypt32 במערך הסייבר מסבירים כי מקור הפגיעויות נמצא ברכיב הקריפטוגרפי קריפטוגרפיים. הפגיעות מאפשרת הטעיה של מערכת ההפעלה והמשתמש בנוגע לאותנטיות של תעודה דיגיטלית או מסר קריפטוגרפי המוצג להם.

רמת החומרה של הפגיעות נובעת מכך שהפגיעות ניתנת לניצול באמצעות זיוף חתימה דיגיטלית על קבצים, לדוגמה, חתימה על קובץ ריצה עוין באמצעות חתימה הנחזית כזו של חברת מיקרוסופט.

במערך הסייבר מציינים כי לעיתים מערכות אבטחה מוגדרות כך שזיהוי קבצים כחתומים על ידי מיקרוסופט, גורם לבדיקה פחות מחמירה של הקבצים או לדילוג על הבדיקה כלל.

כמובן שניתן להסתייע במרכז המבצעי של מערך הסייבר בחיוג ישיר 119.

ביזנעס

שתף כתבה זו

כתבות נוספות במדור טכנולוגיה