26 אפריל 2020
ב' אייר תש"פ
סימוכין:ב-ס-1068

פגיעות במוצר FortiMail

תקציר

לאחרונה דווחה חברת פורטינט על פגיעות במוצר FortiMail.
מומלץ לבחון העדכונים ולהתקינם בהקדם האפשרי.

פרטים

1. זוהתה פגיעות במנגנון ההזדהות של המוצר. בגרסאות מסוימות, תוקף מרוחק שאינו מזוהה יכול להזדהות כמשתמש לגיטימי תוך ניצול המנגנון להחלפת סיסמה.
2. הגרסאות הפגיעות הן:

FortiMail versions 5.4.1 to 5.4.10

FortiMail versions 6.0.0 to 6.0.7

FortiMail versions 6.2.0 to 6.2.2

3. גרסאות המוצר 5.3 וקודמות לה אינן פגיעות.
4. הפגיעות קיבלה את הזיהוי CVE-2020-9294.
5. הפגיעות חשופה רק דרך ממשק הניהול, ולא דרך ממשק המשתמש הרגיל.

דרכי התמודדות

1. מומלץ לבחון העדכונים במערכותיכם ולהתקינם בהקדם האפשרי.
2. הגרסאות העדכניות הן:

FortiMail versions 5.4.11 or above

FortiMail versions 6.0.8 or above

FortiMail versions 6.2.3 or above

3. החל מגרסה 6.0, ניתן לנטרל ממשק הניהול בממשקים השונים לציוד באופן פרטני. ראו ההגדרות בתפריט Network > Interface > Edit Interface> Advanced Setting > Web Access. מומלץ לנטרל ממשק הניהול בממשקים הפונים לרשת האינטרנט.
4. בגרסה 5.4 ניתן לנטרל הגישה ל- URL "/admin" ברגל הנגישה לאינטרנט באמצעות WAF.
5. מומלץ לנטרל את חשבון הניהול המובנה בציוד ולהגדיר חשבונות ניהול לכל מנהלן, או הזדהות באמצעות ממשק חיצוני כגון LDAP או RADIUS.

לכל מידע נוסף ניתן לפנות אלינו. במידה שעלו ממצאים בבדיקתכם, נבקש לקבל היזון חוזר.

מקורות

שיתוף מידע עם ה-CERT הלאומי אינו מחליף חובת דיווח לגוף מנחה כלשהו, ככל שחלה על הגוף חובה כזו.
המידע נמסר כפי שהוא (as is), השימוש בו הוא באחריות המשתמש ומומלץ להיעזר באיש מקצוע בעל הכשרה מתאימה לצורך הטמעתו.

בברכה,
CERT-IL