04 יולי 2020
י"ב תמוז תש"פ
[עדכון]
05 יולי 2020
י"ג תמוז תש"פ
סימוכין:ב-ס-1110C

[עדכון] פגיעויות קריטיות ב-BIG-IP של חברת F5

תקציר

חברת F5 פרסמה לאחרונה מספר עדכוני אבטחה לציוד מסוג BIG-IP מתוצרתה.
2 עדכונים עלולים לאפשר לתוקף לא מזוהה (Unauthenticated) הרצת קוד מרחוק והשתלטות מלאה על הציוד.
מומלץ לבחון ולהתקין העדכונים בהקדם האפשרי.

פרטים

1. מקור הפגיעויות בממשק הניהול של הציוד TMUI (Traffic Management User Interface).
2. הפגיעות החמורה יותר (CVE-2020-5902) קיבלה ציון CVSS 10.0.
3. תוקף עלול לנצל הפגיעות באמצעות משלוח תעבורת HTTP לממשק הניהול. התוצאה עלולה להיות השתלטות מלאה על הציוד או הרצת קוד מרחוק.
4. הפגיעות השנייה (CVE-2020-5903) קיבלה ציון CVSS 7.5.
5. תוקף עלול לנצל פגיעות זו להרצת קוד JavaScript על הציוד בהרשאות המשתמש המחובר לציוד באותה עת. במקרה של משתמש מנהלן בעל הרשאות לממשק ה-Shell של הציוד, המשמעות עלולה להיות הרצת קוד מרחוק.

דרכי התמודדות

1. משתמשים ארגוניים, מומלץ לבחון העדכונים בסביבת ניסוי טרם הטמעה בסביבת ייצור בהקדם האפשרי. גם משתמשים העושים שימוש בגרסה הוירטואלית של התוכנה בסביבת ענן מתבקשים לעדכנה בהקדם האפשרי.
2. הגרסאות העדכניות הן:
    1. 15.1.0.4
    2. 14.1.2.6
    3. 13.1.3.4
    4. 12.1.5.2
    5. 11.6.5.2
3. מומלץ מאד למנוע גישה לממשק הניהול מכתובות שאינן מוכרות, ובפרט מרשת האינטרנט, באמצעות חוקי Firewall או ACL, או באמצעות ההגדרות המפורטות בהתרעות החברה בסעיף "מקורות" להלן.

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

מקורות

1. https://support.f5.com/csp/article/K52145254
2. https://support.f5.com/csp/article/K43638305