8 אוגוסט 2018
כ"ז אב תשע"ח
סימוכין: ב-ס-693

פגיעות במערכת הפעלה לינוקס עלולה לאפשר תקיפת מניעת שירות

תקציר

ניתן לגרום מתקפת מניעת שירות למערכות לינוקס בגרסאות KERNEL 4.9 ומעלה, באמצעות אילוץ מערכת ההפעלה לבצע קריאות על כל פאקטה שנשלחת למערכת. התקיפה זכתה לכינוי SegmentSmack .

פרטים

התקיפה מתאפשרת באמצעות משלוח פאקטות אשר מאלצות ביצוע קריאות לפונקציות מערכת בעלות זמן עיבוד ארוך (tcp_collapse_ofo_queue() and tcp_prune_ofo_queue()).
על פי הערכה, מספיקות פחות מאלפיים פאקטות לשנייה על מנת שהתקיפה תוכתר בהצלחה.
על מנת לבצע את התקיפה התוקף חייב להיות מקושר באמצעות קשר TCP דו-כיווני (כלומר, לא ניתן לשלוח תעבורה מכתובות מזויפות) עם השרת המותקף, בפורט שנגיש לתעבורת TCP.
גרסאות קודמות ל- 4.9 אינן פגיעות.

דרכי התמודדות

ככל שההפצות השונות של לינוקס יוציאו עדכוני אבטחה לפגיעות זו, מומלץ לבחון אותן ולהתקינן במערכותיכם.
מומלץ לתעדף את העדכון לשרתים הנגישים מרשת האינטרנט בפרוטוקולים מבוססי TCP.

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

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

בברכה,
CERT-IL
טל: 9344*
team@cert.gov.il