**מסמך מחקר - ממ״ן 15**

|  |  |
| --- | --- |
| סוג האיום | MITM – men in the middle |
| הרכיב המושפע | ClientLogic |
| שם המודול | Client |
| סיווג החולשה | Håstad broadcast attack+ Cryptographic attack |
| תיאור | החולשה העיקרית נובעת מהדרישה כי בהינתן תשובת כישלון מהשרת הלקוח ישלח את ההודעה עוד פעמיים, כלומר בסה״כ 3 פעמים.  לפי Håstad broadcast attack, כאשר שולח מסויים שולח הודעה לk נמענים שונים כאשר לכולם אותה חזקה ציבורית e ומודולו שונה, לפי מודל התקיפה ברמה ש- k>=3 הצופן בעזרתו הצפינו את ההודעה ניתן לפיענוח.  היות ומפתח הaes מפתח קטן יחסית (128 סיביות) וגם המפתח הציבורי הנוצר הוא מפתח קטן יחסית, יחסית ניתן יותר בקלות לחשב את החזקה הציבורית e בעזרת שיטת קופרסמית׳ (coppersmith method) |
| תוצאה | פגיעה בפרטיות הלקוח |
| דרישות מקדימות | האזנה לport ול-ip של השרת, הכרת מבנה ההודעות ויכולת התחזות מלאה מתחילת הקמת התקשורת (כיוון שהחלפת המפתחות קוראת רק בהתחלה) או כוח עיבוד גבוהה ומהיר יחסית |
| השפעה עסקית | חמורה |
| תיקון מוצע | שימוש בריפוד רנדומלי של התוכן בעת קריאתו ולא רק בסוף או בהתחלה כמו שמבוצע כיום.  שימוש במפתחות ארוכים יותר (מפתח פרטי 4096 סיביות ו-256 סיביות עבור המפתח הסימטרי).  בהינתן כישלון בחישוב ה- crc בצד השרת עליו לייצר מפתח סימטרי חדש, להצפין אותו עם המפתח הציבורי של הלקוח ולשלוח ללקוח יחד עם תשובה הכישלון, ועל הלקוח במצב זה להצפין את התוכן מחדש עם המפתח החדש. |
| סיכון | פוטנציאל נזק: 9  יכולת שיחזור: 7  יכול לממש את התקיפה: 4  לקוחות מושפעים: 8  יכולת גילוי הפרצה: 9  סהכ: 7.2 |