| **Threat** | **ארך מפתח RSA חלש** |
| --- | --- |
| **Affected component** | מנגנון ההצפנה הסימטרי |
| **Module details** | RSAWrapper.cpp |
| **Vulnerability class** | חולשת קריפטוגרפיה |
| **Description** | המערכת מייצרת מפתחות RSA באורך 1024 ביט שכיום מחשבים לפחות מאובטחים לעומת מפתחות באורך 2048 ביט ומעלה. |
| **Result** | תוקף בעל משאבים מספקים עלול לפרק את המפתחות (לחשב את המפתח הפרטי מתוך המפתח הציבורי). |
| **Prerequisites** | על התוקף להיות בעל גישה למשאבי מחשוב גבוהים למשל לצורך שימוש ב GNFS כדי לפרק את המפתחות. בנוסף נדרשת נכונות להשקעת זמן רב בתהליך הפירוק. |
| **Business impact** | ניצול החולשה עלול להוביל לפעולות לא מורשות במערכת, מה שיכול לפגוע בתוכנית ולהביא לחשיפת נתונים רגישים. בנוסף, יכול להיגרם אובדן אמון מצד המשתמשים \ תביעות על פגיעה בפרטיות. |
| **Proposed remediation** | להגדיל את גודל המפתח ל 2048 ביט לפחות כדי להבטיח עמידות גבוהה יותר בפני התקפות פירוק מפתחות. |
| **Risk** | **Damage potential:** 9  **Reproducibility:** 2  **Exploitability:** 3  **Affected users:** 7  **Discoverability:** 6  **Overall:** 5.4 |

| **Threat** | **שימוש ב IV קבוע בהצפנה AES** |
| --- | --- |
| **Affected component** | מודול ההצפנה |
| **Module details** | AESWrapper.cpp, AESWrapper.h |
| **Vulnerability class** | יישום הצפנה חלש |
| **Description** | בכל קריאה לפונקציית ההצפנה והפענוח, נעשה שימוש ב IV מאופס (zeros) במקום ב IV אקראי מה שמקטין את אקראיות ההצפנה. |
| **Result** | התוקף יכול לנתח את התבניות החוזרות בהודעות המוצפנות מה שעלול להביא לחשיפת מידע או אפילו שחזור של המפתח הסימטרי וחשיפת כלל התקשורת. |
| **Prerequisites** | על המערכת להשתמש באותו מפתח עבור מספר הודעות כאשר בכולן נעשה שימוש באותו IV. התוקף צריך להיות מסוגל להאזין לתקשורת המוצפנת למשל על ידי מימוש Man in the Middle. |
| **Business impact** | ניצול החולשה עלול להוביל לחשיפת הודעות או חשיפת התקשרות מלאה, מה שיכול לפגוע תוכנית ולהביא לחשיפת נתונים רגישים. אלה עלולים להוביל לפגיעה במוניטין והוצאות נוספות עבור העסק. |
| **Proposed remediation** | לייצר IV אקראי בכל הצפנה, לצרף אותו יחד עם ההודעה ולוודא שימוש ב IV ייחודי לכל פעולה. |
| **Risk** | **Damage potential:** 9  **Reproducibility:** 2  **Exploitability:** 3  **Affected users:** 7  **Discoverability:** 6  **Overall:** 5.4 |

| **Threat** | **Man-in-the-Middle** |
| --- | --- |
| **Affected component** | תהליך החלפת מפתחות. |
| **Module details** | RSAWrapper.cpp / Client.senSymetricKey |
| **Vulnerability class** | העדר אימות הדדי. |
| **Description** | תהליך ההחלפה של מפתחות AES מתבצע באמצעות הצפנת המפתח על ידי RSA אך ללא אימות הדדי של המפתחות הציבוריים. זה מאפשר לתוקף ליירט את ההחלפה. |
| **Result** | פענוח או שינוי תוכן הודעות וחדירה לתקשורת מוצפנת ושליטה מלאה על זרימת התקשורת בין משתמשים. |
| **Prerequisites** | נדרשת גישה לרשת, כלים ותוכנות ליירוט וניטור תעבורת הרשת והיכרות עם הפרוטוקול. |
| **Business impact** | ניצול החולשה עלול להוביל לגניבת מידע רגיש, שינוי תוכן הודעות, או יצירת גישה למידע מוצפן. מה שיכול לפגוע בשירות המאובטח ולהביא לחשיפת נתונים רגישים. בנוסף, יכול להיגרם אובדן אמון במערכת ואי עמידה בשירות שהיא מציעה. |
| **Proposed remediation** | יישום של אימות הדדי למשל חתימות דיגיטליות \ שימוש בתעודות בתהליך החלפת המפתחות \ התקשרות בערוץ מאובטח. |
| **Risk** | **Damage potential:** 9  **Reproducibility:** 6  **Exploitability:** 7  **Affected users:** 8  **Discoverability:** 6  **Overall:** 7.2 |

| **Threat** | **DoS והזנת קלט עצום** |
| --- | --- |
| **Affected component** | יצירת התקשרות. |
| **Module details** | Connection\_handler.py / handle / client\_socket.recv(1024) |
| **Vulnerability class** | מניעת שירות. |
| **Description** | קריאה קבועה ל recv(1024) ללא מנגנון הגבלת קצב או בדיקת גודל הקלט עלולה לאפשר לשלוח כמויות עצומות של נתונים. |
| **Result** | עומס יתר, האטה או קריסת השרת. |
| **Prerequisites** | נדרשת גישה לרשת ויכולת להתחבר לשרת. יכולת לייצר כמות נתונים גדולה בו זמנית על ידי חיבורים רבים או שליחת כמויות גדולות של מידע במקביל. |
| **Business impact** | ניצול החולשה עלול להוביל לפגיעה באופן שבו פועלת המערכת, ולהביא לאובדן אמון במערכת ואי עמידה בשירות שהיא מציעה, אי זמינות המערכת למשתמשים ועלויות נוספות לעסק. |
| **Proposed remediation** | להגביל את גודל הקלט לכל הודעה, לבצע בדיקות קלט לפני עיבודו. ניתן ליישם מנגנון Rate limiting לחיבורי timeout. |
| **Risk** | **Damage potential:** 6  **Reproducibility:** 8  **Exploitability:** 8  **Affected users:** 10  **Discoverability:** 6  **Overall:** 7.6 |

| **Threat** | **Binding to all network interfaces (0.0.0.0)** |
| --- | --- |
| **Affected component** | האזנת השרת לרשת. |
| **Module details** | Server\_utils.py / init\_server\_socket |
| **Vulnerability class** | גישה בלתי מורשית לשרת. |
| **Description** | השרת נקשר לכתובת 0.0.0.0 ומאזין לכל הממשקים הזמינים מה שמגדיל את שטח ההתקפה ומאפשר גישה מכל כתובת IP ברשת. |
| **Result** | גישה בלתי מורשית, מתקפות מרחוק, מתקפות DoS. |
| **Prerequisites** | נדרשת גישה לרשת ויכולת להתחבר לשרת. |
| **Business impact** | ניצול החולשה עלול להוביל לשיבוש השירות, אי זמינות המערכת למשתמשים או חשיפת נתונים ומכך עלולות לנבוע עלויות נוספות לעסק ופגיעה במוניטין. |
| **Proposed remediation** | להגביל את הקשירה לכתובת IP ספציפית ולהשתמש בחומת אש ובבקרת גישה כדי להגן על השרת. |
| **Risk** | **Damage potential:** 8  **Reproducibility:** 8  **Exploitability:** 9  **Affected users:** 10  **Discoverability:** 5  **Overall:** 8 |