



25.86x31.49	1	6	עמוד	הארץ - מגזין ענן	23/08/2020	74192111-6
קלווטי - חברת טייב - 21452						

אבטחת רשתות בקרה תעשייתיות בעבודה מרחוק

בחודשים האחרונים גילו חוקרי חברת קלארוטי חולשות אבטחה במספר יישומי VPN, המשמשים בעיקר למתן גישה מרחוק לרשתות טכנולוגיות תפעוליות (OT). מהן אותן חולשות, כיצד ניתן להתמודד עימן ומה מבשר שיתוף הפעולה של החברה עם צ'ק פוינט בתחום אבטחת רשתות בקרה תעשייתיות?

נדב בית הלחמי



תוקפים שמתמקדים ב-VPN. כלים אלה מאפשרים לארגונים להתחבר דרך חיבור מוצפן לשרת, כאשר לאחר מכן השרת מעביר את התקשורת לרשת הפנימית. משמעות הרבר היא שהשרת הוא נכס קריטי ברשת מכיוון שיש לו "רגל" אחת באינטרנט, נגישה לכולם, ו"רגל" נוספת ברשת הפנימית המאובטחת. המשמעות - מעקף לכל אמצעי האבטחה ההיקפיים. לפיכך, קבלת גישה אליו יכולה לאפשר לתוקפים לא רק לקבל יכולת תנועה פנימית, אלא גם להתנגח כאילו הם אורחים לגיטימיים ברשת.

בשנים האחרונות ראינו מעבר לפתרונות גישה מרחוק מבוססי ענן, המאפשרים בדרך כלל פריסה מהירה ומפחיתים את העלויות. בדרך כלל הם מצייעים גם פתרונות "מוצר מרובה" (white-label) שחברות גדולות יכולות לרכוש כדי שיהיה להם ענן אישי משלהם, על בסיס תוכנה שבסיסה זהה אצל כולם. כפועל יוצא מכך, מציאת באגים במקרה אחר עשויה להשפיע על מקרים אחרים.

Secomea GateManager הוא רוג'אמא אחת שבדקו חוקרי קלארוטי. מדובר בשרת גישה מרחוק ל-ICS הנמצא בשימוש נרחב ברחבי העולם כפתרון SaaS מבוסס ענן למטרות כלליות. על-פי אתר Secomea, שרת הענן של GateManager נועד לספק את הנחיות של גישה מהירה וקלה לאינטרנט, תוך הימנעות מהגדרות שרת מסוככות. שרון ברויזינב ומל קרן מצוות המחקר של קלארוטי, גילו כי שרת זה מכיל פגמי אבטחה מרובים, כולל פגיעות קריטיות שמשפיעה על רכיב GateManager, שהוא הניתוב העיקרי בפתרון הגיי-שה המרוחקת של Secomea. רכיב GateManager GateManager ממוקם בקצה הרשת הארגונית וחשוף לרשתות חיצוניות כמו האינטרנט, כאשר הוא מקבל את החיבור מאתרים מרוחקים. שרתי ענן מסוג זה הם מרובי משתמשים (multi-tenant) ומספקים שירות למספר ארגונים שונים במקביל. לכן, השתלטות על שרת כזה תוביל לחרידה פוטנציאלית בכלל הארגונים המשתמשים בשרת ענן זה.

המעבר לעבודה מרחוק בימי הקורונה הזניק את השימוש ב-VPN. מחקר של חברת הסייבר התעשייתי קלארוטי (Claroty) מראה שהפתרונות הטכנולוגיים המובילים כיום בשוק לעבודה מרחוק, עבור מפעלים ותשתיות קריטיות, פגיעים למגוון התקפות סייבר, אשר מאפשרות לתוקפים לחדור פנימה לרשתות הקריטיות של הארגונים.

בחודשים האחרונים גילו חוקרי חברת קלארוטי חולשות אבטחה במספר יישומי VPN (רשת פרטית וירטואלית), המשמשים בעיקר למתן גישה מרחוק לרשתות טכנולוגיות תפעוליות (OT). פתרונות ייעודיים אלה לגישה מרחוק מתמקדים בעיקר ברענן מערכות הבקרה התעשייתיות (SCADA) השימוש העיקרי בהם הוא לאפשר תחזוקה ופיקוח מרחוק על בקרי שטח ומכשור, כולל בקרי לוגיקה ניתנים לתכנות (PLC) והתקני קלט/פלט (IO). ניי צול חולשות אלה יכול לתת לתוקפים גישה ישירה למכשור בשטח ולגרום אפילו לנוק פייז.

המוצרים הפגיעים נמצאים בשימוש נרחב בתעשיות כמו נפט וגז, שירותי מים וחשמל, בהן הקריטיות המאובטחת אתרים מרוחקים היא קריטית. מלבד קישוריות בין אתרים, פתרונות לגישה מרחוק אף מאפשרים למפעלים מרחוק ולספקי צד ג' לחייג לאתרי לקוחות ולספק תחזוקה ופיקוח. הגישה מרחוק קיבלה עדיפות מיוחדת בחודשים האחרונים בגלל המציאות החדשה שהביאה עמה מגפת הקורונה.

רגל פה, רגל שם

כדי להבין טוב יותר את הסיכון הנובע מניצול של חולשות אלה, ומה ניתן לעשות כדי להתגונן מפני התקפות מסוג זה, צוות המחקר של קלארוטי בחן בהרחבה את רמת האבטחה של מספר פתרונות פופולריים לגישה מרחוק. הממצאים שעלו מהחישו, כי שרתי גישה מרחוק פגיעים במספר דרכים שונות, ועלולים לשמש כאתרי התקפה יעילים ביותר עבור

הגדרשת להגנה מפני מתקפות סייבר על רשתות OT ומערכת בקרה תעשייתית (ICS). כשחופה טכנולוגית של צ'ק פוינט, קלארוטי תומכת בגילוי ובסיווג של מכשירי OT במגוון ענפי תעשייה, ובכך מעניקה ללקוחות צ'ק פוינט פתרון אבטחה משולב מקצה לקצה. "אנו שמחים לשלב את קלארוטי בתוכנית IoT Protect Discovery של צ'ק פוינט", אמר ראם שפר, מנהל מוצר בצ'ק פוינט. "השילוב של הפתרון לזיהוי איומים מתמשכים של קלארוטי (CTD) ופתרון מניעת האיומים IoT Protect של צ'ק פוינט, מספק ללקוחות התעשייתיים את הנדרשות האבטחה והאוטומציה הנדרשים להגנה על רשתות מפני איומי IoT".

עמנואל סלמונה, סמנכ"ל שותפות גלובליות בקלארוטי, אמר כי "צ'ק פוינט היא מספקות הפיידול המבוססות ביותר, עם מיצוב ונתח שוק משי מעתיים, ולכן השותפות עימה פותחת עבור קלארוטי ערוץ חשוב לשוק, ואנו נרשמים מההזדמנות להרחיב יחד אתם את ההיצע הטכנולוגי שלנו".

השותפות בנויה על אינטגרציה בין פתרון זיהוי האיומים של קלארוטי (CTD - Continuous Threat Detection) ופתרון IoT Protect של צ'ק פוינט. התראות האבטחה של פלטפורמת קלארוטי נשלחות ל-Manager IoT Protect Controller של צ'ק פוינט, אשר קובע את מדיניות האבטחה שנאכפת באמצעות Quantum Security Gateways של צ'ק פוינט. רוח אבטחה מאחד מאפשר לארגונים לראות כל איום על יישום, תהליך או רשת, ומספק ניראות מלאה של הארגון ורשתות הבקרה.

הבאג שהתגלה מתרחש עקב טיפול שגוי בדרך בה השרת מטפל בקבלת תקשורת מסוג מסוים. השרת בר מאפשר לתוקף לגשת מרחוק ל-GateManager ללא צורך בשם משתמש או סיסמה. התקפה כזו, אם מצליחה, עלולה לגרום לפריצת אבטחה מוחלטת המעניקה לתוקפים גישה מלאה לרשת הפנימית של כל הלקוחות המשתמשים בשרת ענן, יחד עם היכולת לפענח את כל התעבורה ב-VPN. חוקרי קלארוטי הודיעו לראשונה ל-Secomea על חולשה זו ב-26 במאי 2020, והחברה דאגה לתיקון ב-10 ביולי 2020.

אבטחה ונראות לתשתיות קריטיות

קלארוטי משפרת את הזמינות, הבטיחות והאמינות של נכסי ה-OT ורשתות ה-OT במפעים תעשייתיים ובתשתיות קריטיות. שלא כמו פתרונות נישא - המוגבלים לגילוי OT פסיבי בלבד, גישה מרחוק מבוססת VPN, או פלטפורמות IoT שאינן נותנות מענה מלא לכל צורכי ה-OT - הפלטפורמה של קלארוטי מספקת נראות OT מקיפה, פילוח, ניהול פגיעויות, זיהוי איומים, הערכת סיכונים ויכולות לאבטחת הגישה מרחוק (Secure Remote Access - SRA) וכל זאת במסגרת פתרון אחד, נטול סוכן. פתרון זה נתמך בצוות מחקר אבטחת ה-OT של קלארוטי ומערך האינטגרציה הרחב שלה.

לאחרונה חתמה החברה על הסכם שיתוף פעולה עם צ'ק פוינט, במטרה לספק לארגונים ולמפעילי תשתיות קריטיות אבטחה וניראות בזמן אמת, ברמה

באג שגילו החוקרים של קלארוטי מאפשר לתוקפים לגשת לשרת הגישה-מרחוק ללא צורך בשם משתמש או סיסמה. התקפה כזו, אם מצליחה, עלולה לגרום לפריצת אבטחה מוחלטת המעניקה לתוקפים גישה מלאה לרשת הפנימית של כל הלקוחות המשתמשים בשרת ענן, יחד עם היכולת לפענח את כל התעבורה ב-VPN