วันที่ 25 กันยายน 2569

ช่องโหว่ OnePlus ที่ยังไม่ได้รับการแก้ไข เปิดทางให้แอป Android ที่ติดตั้งอยู่สามารถเข้าถึงสิทธิ์ Root ได้โดยไม่ต้องขอ Permission

สมาร์ตโฟน OnePlus 15 ที่ใช้ OxygenOS เวอร์ชันล่าสุด สามารถถูก Root ได้โดยแอปที่เป็นอันตรายซึ่งผู้ใช้ติดตั้งลงในเครื่อง โดยแอปดังกล่าวไม่จำเป็นต้องขอสิทธิ์พิเศษใดๆ จากผู้ใช้ นักวิจัยด้านความปลอดภัย Rasmus Moorats พบว่าสามารถนำช่องโหว่ 2 รายการในซอฟต์แวร์ของ OnePlus มาเชื่อมต่อกัน เพื่อเข้าถึงสิทธิ์ Root ซึ่งเป็นระดับสิทธิ์สูงสุดในการควบคุมโทรศัพท์ Android โหว่ลักษณะเดียวกันนี้ส่งผลกระทบต่ออุปกรณ์ของ OnePlus อีกหลายรุ่น รวมถึงอุปกรณ์ของ OPPO ด้วย แต่บริษัทไม่ได้ระบุว่ามีรุ่นใดบ้างที่ได้รับผลกระทบ

OnePlus ยืนยันช่องโหว่ทั้งสองรายการในเดือนพฤษภาคมที่ผ่านมา และในคำตอบเดียวกัน บริษัทระบุว่า OnePlus เป็นผู้มีสิทธิ์แต่เพียงผู้เดียวในการตัดสินใจว่าจะเปิดเผยข้อมูลช่องโหว่เมื่อใด พร้อมเตือนว่าการเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาตจากบริษัทอาจทำให้ผู้วิจัยต้องรับผิดทางกฎหมาย อย่างไรก็ตาม Moorats ยังคงเผยแพร่รายละเอียดในวันที่ 24 กันยายน ขณะที่ OnePlus ยังไม่ได้ออกแพตช์แก้ไข

OnePlus ได้ชี้แจงจุดยืนของบริษัทไว้ในอีเมลตอบกลับ ซึ่ง Moorats ได้นำมาเผยแพร่แบบเต็มฉบับ โดยระบุว่าบริษัทมีแผนที่จะออกแพตช์แก้ไข แต่ยืนยันว่ามีสิทธิ์ขั้นสุดท้ายแต่เพียงผู้เดียวในการเปิดเผยข้อมูลช่องโหว่ และระบุว่าแม้หลังจากมีการออกแพตช์แล้ว นักวิจัยก็ไม่ควรเผยแพร่รายละเอียดทางเทคนิคทั้งหมดด้วยตนเอง

บริษัทให้เหตุผลว่า กฎด้านความมั่นคงปลอดภัยไซเบอร์ของยุโรปกำหนดให้ผู้ผลิตต้องรับรายงานและแก้ไขช่องโหว่ แต่ไม่ได้เปิดทางให้นักวิจัยสามารถเปิดเผยข้อมูลดังกล่าวโดยไม่ได้รับความยินยอมจากผู้ผลิต พร้อมเตือนว่า หากเขาเผยแพร่ข้อมูลโดยไม่ได้รับอนุญาต OnePlus จะดำเนินการทางกฎหมายที่เกี่ยวข้องตามกฎหมายที่บังคับใช้

การโจมตีทำงานอย่างไร

Moorats พบช่องโหว่แรกในบริการของ OnePlus ที่ชื่อว่า AtlasService ซึ่งทำหน้าที่รวบรวมข้อมูลสำหรับการตรวจสอบและแก้ไขปัญหา โดยบริการนี้ทำงานด้วยสิทธิ์ Root และเปิดรับคำสั่งจากแอปใดๆ ก็ได้โดยไม่มีการตรวจสอบว่าแอปที่ส่งคำสั่งเข้ามาคือใคร ผู้โจมตีสามารถสร้างคำสั่งที่ออกแบบมาเป็นพิเศษเพื่อส่งไปยังเครื่องมือสำหรับตรวจสอบปัญหาของ OnePlus ซึ่งเครื่องมือนี้จะนำข้อความที่แอปส่งเข้ามาไปใส่ในคำสั่งระบบโดยไม่มีการตรวจสอบอย่างเหมาะสม ส่งผลให้แอปสามารถได้รับสิทธิ์ Root แต่ยังคงถูกจำกัดอยู่ภายในพื้นที่ระบบที่เรียกว่า dumpstate ซึ่งไม่สามารถทำทุกอย่างได้เหมือน Root ที่มีสิทธิ์เต็มรูปแบบ

ช่องโหว่ที่สองจึงเข้ามาช่วยให้การโจมตีเสร็จสมบูรณ์ OnePlus มีบริการอีกตัวหนึ่งชื่อ olc2 ซึ่งเป็นส่วนช่วยจัดการด้านฮาร์ดแวร์ และมีคำสั่งที่สามารถรันคำสั่ง Shell ใดๆ ที่ได้รับเข้ามาได้ โดยมีการป้องกันเพียงอย่างเดียวคือ ผู้ที่เรียกใช้คำสั่งดังกล่าวต้องมีสิทธิ์ Root อยู่ก่อน ซึ่งเป็นสิทธิ์ที่ช่องโหว่แรกทำให้แอปได้รับมา เมื่อใช้ช่องโหว่ที่สอง คำสั่งจะถูกรันในพื้นที่ระบบที่ให้สิทธิ์ Linux ระดับต่ำทั้งหมด รวมถึงความสามารถในการโหลดโค้ดเข้าสู่ Kernel ทำให้แอปสามารถควบคุมอุปกรณ์ได้ในระดับระบบ

ใครบ้างที่ได้รับผลกระทบ และควรทำอย่างไร

การโจมตีนี้เป็นการโจมตีจากภายในอุปกรณ์ โดยแอปที่เป็นอันตรายจะต้องถูกติดตั้งและทำงานอยู่บนโทรศัพท์ก่อนจึงจะสามารถเริ่มการโจมตีได้ ไม่สามารถโจมตีโทรศัพท์ผ่านอินเทอร์เน็ตโดยตรงได้ อย่างไรก็ตาม เมื่อแอปดังกล่าวถูกติดตั้งแล้ว แอปไม่จำเป็นต้องขอ Permission ใดๆ และจะไม่แสดงหน้าต่างแจ้งเตือนให้ผู้ใช้อนุญาต อีกทั้งการโจมตีนี้ยังสามารถทำงานได้บนโทรศัพท์ที่ใช้ซอฟต์แวร์จากโรงงานโดยไม่ได้มีการดัดแปลงระบบ ซึ่งในขณะนี้ยังไม่มีหลักฐานว่าช่องโหว่ดังกล่าวถูกนำไปใช้โจมตีจริงในวงกว้าง

Moorats ยังยืนยันว่าการโจมตีสามารถทำงานได้บน OnePlus 12 Pro รุ่นเก่า และคาดว่าปัญหาเดียวกันอาจเกิดขึ้นกับอุปกรณ์ที่ใช้ OxygenOS 16 ในวงกว้าง เนื่องจาก OnePlus และ OPPO พัฒนาซอฟต์แวร์พื้นฐานร่วมกัน จึงเป็นเหตุผลที่คำเตือนของ OnePlus ครอบคลุมถึงอุปกรณ์ของ OPPO ด้วย

ในวันที่ Moorats เปิดเผยข้อมูล OnePlus ยังไม่ได้กำหนดหมายเลข CVE ให้กับช่องโหว่ดังกล่าว และยังไม่มีแพตช์แก้ไข รวมถึงยังไม่พบประกาศด้านความปลอดภัยจาก OnePlus ที่ระบุรายละเอียดของช่องโหว่นี้โดยตรง ดังนั้นจนกว่าจะมีการออกแพตช์ วิธีป้องกันที่ทำได้ในทางปฏิบัติคือ ติดตั้งแอปเฉพาะจากแหล่งที่เชื่อถือได้ เนื่องจากการโจมตีนี้ไม่สามารถเริ่มต้นได้หากไม่มีแอปที่เป็นอันตรายติดตั้งอยู่บนโทรศัพท์

ตามข้อมูลของ Moorats กระบวนการเปิดเผยช่องโหว่ใช้เวลาประมาณ 5 เดือน โดยมีไทม์ไลน์ดังนี้

- **18 เมษายน 2026:** รายงานช่องโหว่ทั้งสองรายการให้ OnePlus ทราบ
- **20 พฤษภาคม:** OnePlus ยืนยันว่าช่องโหว่มีอยู่จริง พร้อมระบุว่าบริษัทเป็นผู้มีสิทธิ์ควบคุมการเปิดเผยข้อมูลแต่เพียงผู้เดียว และเตือนถึงความรับผิดทางกฎหมายหากเขาเผยแพร่ข้อมูล

- **22 มิถุนายน:** OnePlus แจ้งความคืบหน้าเกี่ยวกับการแก้ไขช่องโหว่ และขอให้เขาชะลอการเผยแพร่ข้อมูล ซึ่งเขาตกลงว่าจะยังไม่เผยแพร่ก่อนวันที่ 17 กันยายน
- **20 กรกฎาคม และ 11 กันยายน:** เขาติดต่อ OnePlus เพื่อขอข้อมูลอัปเดต แต่ไม่ได้รับการตอบกลับ
- **24 กันยายน:** เขาเผยแพร่รายละเอียดของช่องโหว่

นอกจากนี้ เหตุการณ์ดังกล่าวไม่ใช่กรณีแรกในช่วงที่ผ่านมา ที่แอปซึ่งติดตั้งอยู่บนโทรศัพท์ Android สามารถเข้าถึงสิทธิ์ Root ได้ ในเดือนสิงหาคม Lukas Maar นักวิจัยจากบริษัทด้านความปลอดภัย Calif เปิดเผยเทคนิคอีกวิธีหนึ่ง ซึ่งสามารถทำให้แอปที่ไม่ต้องขอ Permission ใดๆ ได้รับสิทธิ์ Root บนโทรศัพท์ที่ยังล็อกอยู่และใช้เฟิร์มแวร์เวอร์ชันล่าสุดจาก Samsung, Xiaomi, OPPO, OnePlus และ Realme โดยอาศัยช่องโหว่ในโค้ดที่ผู้ผลิตแต่ละรายเพิ่มเข้ามาในระบบ Android

ก่อนหน้านี้ OnePlus ก็เคยใช้เวลานานในการตอบกลับนักวิจัยเช่นกัน โดยในปี 2025 Rapid7 รายงาน ถึงช่องโหว่ใน OxygenOS อีกหนึ่งรายการ ซึ่งเปิดทางให้แอปใด ๆ สามารถอ่านข้อความของผู้ใช้ได้ และระบุว่า OnePlus ไม่ได้ตอบกลับจนกว่าข้อมูลการวิจัยดังกล่าวจะถูกเผยแพร่สู่สาธารณะ

ข้อมูลอ้างอิง

Sep 24, 2026 By Ravie Lakshmanan

- https://thehackernews.com/2026/09/unpatched-oneplus-flaws-let-installed.html