วันที่ 8 กรกฎาคม 2569

ผู้โจมตีเริ่มสแกนหาและทดสอบช่องโหว่ Gitea Docker CVE-2026-20896 เพียง 13 วันหลังเปิดเผยข้อมูล

บริษัทด้านความมั่นคงปลอดภัยบนคลาวด์ Sysdig เปิดเผยว่า พบผู้ไม่หวังดีเริ่มพยายามโจมตีช่องโหว่ร้ายแรงที่เพิ่งได้รับการแก้ไขใน Docker Image ของ Gitea หลังจากมีการเปิดเผยข้อมูลช่องโหว่สู่สาธารณะได้เพียง 13 วัน

ช่องโหว่ดังกล่าวคือ CVE-2026-20896 ซึ่งมีคะแนนความรุนแรง CVSS 9.8 โดยเกิดจากแพลตฟอร์ม DevOps ของ Gitea เชื่อถือค่า Header "X-WEBAUTH-USER" จากทุกแหล่งที่มา ทำให้ผู้โจมตีจากอินเทอร์เน็ตสามารถยกระดับสิทธิ์และเข้าสู่ระบบได้โดยไม่ต้องยืนยันตัวตน

ในแถลงการณ์ที่ส่งให้ The Hacker News ทางอีเมล Ali Mustafa (@rz1027) นักวิจัยด้านความมั่นคงปลอดภัย ผู้ค้นพบและรายงานช่องโหว่นี้ ระบุว่า Docker Image ของ Gitea มาพร้อมกับไฟล์ Template "app.ini" ที่กำหนดค่า * "REVERSE_PROXY_TRUSTED_PROXIES = " ไว้เป็นค่าเริ่มต้น โดยไฟล์ app.ini เป็นไฟล์กำหนดค่าหลักของ Gitea ที่ใช้จัดการการตั้งค่าเซิร์ฟเวอร์ การเชื่อมต่อฐานข้อมูล พฤติกรรมด้านความปลอดภัย และการตั้งค่าต่างๆ ของแอปพลิเคชัน

เมื่อเปิดใช้งานการล็อกอินผ่าน Reverse Proxy การใช้เครื่องหมายดอกจัน (*) จะหมายถึงการเชื่อถือทุก Source IP ดังนั้นใครก็ตามที่สามารถเข้าถึงพอร์ตของ Gitea ได้ ก็สามารถส่ง Header X-WEBAUTH-USER เพื่อปลอมตัวเป็นผู้ใช้รายใดก็ได้โดยไม่ต้องใช้รหัสผ่านหรือ Token" Mustafa อธิบาย "หากเปิดใช้งานการสร้างบัญชีผู้ใช้อัตโนมัติ (Auto-registration) การระบุชื่อบัญชีผู้ดูแลระบบก็จะทำให้ได้รับสิทธิ์ผู้ดูแลระบบทันที

ทั้งนี้ ค่าเริ่มต้นที่ปลอดภัยของตัวแปร REVERSE_PROXY_TRUSTED_PROXIES ตามเอกสารของ Gitea คือ "127.0.0.0/8,::1/128" ซึ่งอนุญาตให้เฉพาะ Localhost หรือ Loopback Interface เท่านั้นที่สามารถทำหน้าที่เป็น Reverse Proxy ที่เชื่อถือได้

อย่างไรก็ตาม Docker Image อย่างเป็นทางการของ Gitea ไม่ได้ใช้ค่าดังกล่าว แต่กลับกำหนดค่าเป็น "*" ซึ่งหมายถึงการยอมรับทุก IP Address ส่งผลให้การตรวจสอบ Allowlist แทบไม่มีประโยชน์

ด้วยเหตุนี้ หากผู้ดูแลระบบเปิดใช้งานตัวเลือก "ENABLE_REVERSE_PROXY_AUTHENTICATION = true" เพื่อใช้งาน Gitea ผ่าน Reverse Proxy สำหรับยืนยันตัวตน แต่ยังคงใช้ค่าเริ่มต้นของ REVERSE_PROXY_TRUSTED_PROXIES ระบบจะยอมรับ Header X-WEBAUTH-USER จากทุก Source IP ที่สามารถเข้าถึง Container ได้

คำแนะนำด้านความปลอดภัยของ Gitea ระบุว่า ทุกโปรเซสที่สามารถเชื่อมต่อมายัง HTTP Port ของ Gitea ได้โดยตรง โดยไม่ผ่าน Reverse Proxy ที่ใช้ยืนยันตัวตน สามารถปลอมตัวเป็นผู้ใช้รายใดก็ได้ หากทราบหรือสามารถเดาชื่อบัญชีผู้ใช้นั้นได้ โดยบัญชีผู้ดูแลระบบ เช่น admin, gitea_admin และชื่ออื่นๆ ในลักษณะเดียวกัน ถือเป็นเป้าหมายหลัก

ช่องโหว่นี้ส่งผลกระทบต่อ Docker Image ของ Gitea ตั้งแต่เวอร์ชันก่อน 1.26.2 และรวมถึง 1.26.2 โดยได้รับการแก้ไขแล้วในเวอร์ชัน 1.26.3 ที่เผยแพร่เมื่อช่วงปลายเดือนที่ผ่านมา ซึ่งได้ลบการกำหนดค่า "*" ออกจากค่าเริ่มต้น และเปลี่ยนให้การใช้งาน Reverse Proxy Authentication ต้องเปิดใช้งานด้วยตนเอง (Opt-in)

ต่อมา Sysdig เปิดเผยว่า พบความพยายามโจมตีช่องโหว่นี้จริงบนอินเทอร์เน็ต (In-the-Wild) เป็นครั้งแรก หลังจากมีการเปิดเผยข้อมูลสู่สาธารณะเพียง 13 วัน โดยปัจจุบันมีเซิร์ฟเวอร์ Gitea ที่เปิดให้เข้าถึงจากอินเทอร์เน็ตประมาณ 6,200 เครื่อง

"จนถึงขณะนี้ กิจกรรมที่พบยังอยู่ในขั้นตอนของการสำรวจและตรวจสอบระบบโดยผู้โจมตี" Michael Clark ผู้อำนวยการอาวุโสฝ่ายวิจัยภัยคุกคามของ Sysdig กล่าวกับ The Hacker News

"แม้เราจะพบการเชื่อมต่อครั้งแรกจาก IP ของบริการ ProtonVPN หมายเลข 159.26.98[.]241 แต่จนถึงตอนนี้ยังไม่พบการพัฒนาไปสู่การโจมตีหรือการใช้ประโยชน์จากช่องโหว่อย่างเต็มรูปแบบ เราเชื่อว่าเราตรวจพบเหตุการณ์นี้ได้ตั้งแต่ระยะเริ่มต้นก่อนที่ผู้โจมตีจะมีโอกาสขยายการโจมตีต่อ"

เนื่องจากช่องโหว่นี้มีความรุนแรงในระดับสูง ผู้ใช้งานและผู้ดูแลระบบจึงควรอัปเดต Gitea Docker Image เป็นเวอร์ชันล่าสุดโดยเร็วที่สุด เพื่อป้องกันความเสี่ยงจากการถูกโจมตี

ข้อมูลอ้างอิง

Jul 6, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/threat-actors-probe-gitea-docker-flaw.html