**แจ้งเตือน : ช่องโหว่**

**Nginx LDAP-Auth Daemon Zero Day**

**ผลกระทบทางธุรกิจ**
- ☒ Financial Damage
- ☒ Reputation Damage
- ☐ Non-compliance
- ☐ Privacy Violation

**ผลกระทบต่อระบบ**
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

**TLP Color : White**

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือนช่องโหว่ประเภท Zero-Day สำหรับการพิสูจน์และยืนยันตัวตนผ่านไลบรารี LDAP-Auth Daemon บนซอฟต์แวร์ Nginx สำหรับ Web Service

**วันที่แจ้งเตือน 12 เมษายน 2565**

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับช่องโหว่ประเภท Zero-Day สำหรับการพิสูจน์และยืนยันตัวตนผ่านไลบรารี LDAP-Auth Daemon บนซอฟต์แวร์ Nginx สำหรับ Web Service ทำให้ผู้ไม่หวังดีสามารถใช้เทคนิคการโจมตีโดยแทรกคำสั่งผ่านไลบรารี LDAP-Auth Daemon (LDAP Injection) ส่งผลให้สามารถเรียกใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution)

**นักวิจัยด้านการรักษาความปลอดภัยได้ทำการ Proof of Concept (POC) แล้วพบว่าช่องโหว่ดังกล่าวไม่ซับซ้อนและสามารถใช้งานได้จริงบน Nginx LDAP Reference โดยเวอร์ชันที่ได้รับผลกระทบตั้งแต่เวอร์ชัน 18.1 เป็นต้นมา**

ในปัจจุบันเจ้าของผลิตภัณฑ์ยังไม่ได้มีการออก Security Patch เพื่อแก้ไขช่องโหว่ดังกล่าว เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ผู้ดูแลระบบสามารถใช้วิธีการเพื่อที่จะลดความเสี่ยงเบื้องต้น (Workaround) ดังนี้

   1.1. ตั้งค่ายกเลิกการใช้งานค่าเริ่มต้นของ Parameter ใน Configuration File “nginx-ldap-auth.conf” โดยสามารถศึกษารายละเอียดได้ใน URL ที่อ้างอิง

   1.2. ตรวจสอบให้แน่ใจว่าไม่มีการใช้ Parameter “– ( ) –” หรือ “ = “ ในการเปิดหรือปิดคำสั่งในไลบรารี Backend ของ LDAP-Auth Daemon

2. ติดตามการออก Security Patch อย่างใกล้ชิดเพื่อให้สามารถลดความเสี่ยงที่ใช้ช่องโหว่ดังกล่าวโจมตีองค์กรได้อย่างทันการณ์

3. ผู้ดูแลระบบควรประเมินความเสี่ยงจากการใช้วิธีแก้ไขความเสี่ยงชั่วคราว (Workaround) รวมถึงการตั้งค่าการป้องกันบนอุปกรณ์รักษาความปลอดภัย เพื่อประเมินผลกระทบต่อการทำงานของซอฟต์แวร์ Nginx สำหรับ Web Service ดังกล่าวก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

**แจ้งเตือน : ช่องโหว่**

**Nginx LDAP-Auth Daemon Zero Day**

**ผลกระทบทางธุรกิจ**

- ☒ Financial Damage
- ☒ Reputation Damage
- ☐ Non-compliance
- ☐ Privacy Violation

**ผลกระทบต่อระบบ**

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

**TLP Color : White**

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือนช่องโหว่ประเภท Zero-Day สำหรับการพิสูจน์และยืนยันตัวตนผ่านไลบรารี LDAP-Auth Daemon บนซอฟต์แวร์ Nginx สำหรับ Web Service

วันที่แจ้งเตือน 12 เมษายน 2565

**ข้อมูลอ้างอิง** *External Link*

1) Workaround
   1.1. https://www.nginx.com/blog/addressing-security-weaknesses-nginx-ldap-reference-implementation/?utm_medium=owned-social&utm_source=twitter&utm_campaign=ww-nx_sec_g&utm_content=bg-&fbclid=IwAR3hVNgPGEeroaA1fuVK-0gImX68KsanuXFjblRv4UhHk3GhSAwlDA5-Yvc
   1.2. https://github.com/AgainstTheWest/NginxDay?fbclid=IwAR1gKv1xDS7lFxwB35Tzm-axIXgPZeoRB7vzKmOsmVI-r2ZkzYhy4aXYL-k
2) https://github.com/AgainstTheWest/NginxDay?fbclid=IwAR1gKv1xDS7lFxwB35Tzm-axIXgPZeoRB7vzKmOsmVI-r2ZkzYhy4aXYL-k
3) https://securityonline.info/nginx-zero-day-rce-vulnerability-alert/?fbclid=IwAR0MjXNHONee8TpPor-0SBMEZBB1BSavU0livEdpyWstpDSN1rzr0wEGpiU
4) https://www.cyberkendra.com/2022/04/nginx-release-advisory-about-nginx-0day.html