แจ้งเตือน : ช่องโหว่

HIGH

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ WordPress (CVE-2023-32741) และ ช่องโหว่ Microsoft Exchange Server (CVE-2023-36439)

วันที่แจ้งเตือน 30 พฤศจิกายน 2566

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) [1] สกมช. ตรวจพบข่าวสารบนเว็บไซต์ที่น่าเชื่อถือเกี่ยวกับช่องโหว่หมายเลข **CVE-2023-32741 (ความรุนแรงระดับสูง)** เป็นช่องโหว่ของปลั๊กอิน "Contact Form to Any API" ใน ซอฟต์แวร์ WordPress ซึ่งผู้ไม่หวังดีสามารถโจมตีแบบ SQL Injection ผ่านช่องโหว่ดังกล่าวและเป็นผลให้ผู้ไม่หวังดีอาจได้รับสิทธิระดับสูงในการเข้าถึงระบบและข้อมูลจากฐานข้อมูลได้

เวอร์ชันที่ได้รับผลกระทบ[2] ได้แก่ ปลั๊กอิน WordPress Contact Form to Any API เวอร์ชันตั้งแต่ 1.1.2 และเวอร์ชันก่อนหน้าทั้งนี้ ThaiCERT แนะนำให้ดำเนินการ Update ปลั๊กอิน “Contact Form to Any API” เป็นเวอร์ชันล่าสุดตั้งแต่ 1.1.3 ขึ้นไปทันที [3]

นอกจากนี้ ThaiCERT ยังตรวจพบข่าวสารเกี่ยวกับช่องโหว่หมายเลข **CVE-2023-36439 (ความรุนแรงระดับสูง)** เป็นช่องโหว่ของ Microsoft Exchange Server ที่ผู้ไม่หวังดีที่ผ่านการยืนยันตัวตนบนระบบ Microsoft Exchange Server สามารถใช้ช่องโหว่นี้เพื่อเรียกใช้การควบคุมระบบจากระยะไกล (RCE : Remote code execution) โดยใช้สิทธิการเข้าถึงระดับสูง (NT AUTHORITY\SYSTEM) ทั้งนี้ ช่องโหว่ดังกล่าวถูกใช้เพื่อการโจมตีมากที่สุด ซึ่งได้รับการแก้ไขด้านความปลอดภัยแล้วเมื่อเดือนพฤศจิกายน 2566

เวอร์ชันที่ได้รับผลกระทบ [4] ได้แก่

- Microsoft Exchange Server 2016 Cumulative Update 23 ตั้งแต่ 15.01.0 จนถึงก่อน 15.01.2507.035
- Microsoft Exchange Server ตั้งแต่ 15.02.0 จนถึงก่อน 15.02.1258.028
- Microsoft Exchange Server 2019 Cumulative Update 12 ตั้งแต่ 15.02.0 จนถึงก่อน 15.02.1118.040

ThaiCERT แนะนำให้หน่วยงานที่ใช้ Microsoft Exchange เวอร์ชันที่ได้รับผลกระทบ ดำเนินการตรวจสอบ และ update เป็นเวอร์ชันตามที่ Microsoft แนะนำ [5]

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันอังคารที่ 28 พฤศจิกายน 2566
2) https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/contact-form-to-any-api/contact-form-to-any-api-112-authenticated-administrator-sql-injection
3) https://patchstack.com/database/vulnerability/contact-form-to-any-api/wordpress-contact-form-to-any-api-plugin-1-1-2-sql-injection-vulnerability
4) https://www.cve.org/CVERecord?id=CVE-2023-36439
5) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36439