ด่วนที่สุด

ที่ ศธ ๐๗๐๓๘/ว ๒๔๓๙



สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดชลบุรี
เลขที่ ๙๗/๓๒ หมู่ที่ ๑ ถนนพระยาสัจจา
ตำบลเสม็ด อำเภอเมืองชลบุรี
จังหวัดชลบุรี ๒๐๐๐๐

๖ พฤศจิกายน ๒๕๖๙

เรื่อง การตรวจสอบและแก้ไขช่องโหว่ระดับวิกฤตใน PHP (PHP2Shell)

เรียน ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอเมืองชลบุรี

สิ่งที่ส่งมาด้วย แบบตอบรับการดำเนินการตามแนวทางการป้องกันและลดความเสี่ยงจากช่องโหว่ระดับวิกฤติใน PHP จำนวน ๑ ชุด

ด้วย กรมส่งเสริมการเรียนรู้ แจ้งว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตรวจพบช่องโหว่ระดับวิกฤตใน PHP หรือ PHP2Shell ได้แก่ CVE-2026-109618 และ CVE-2026-109619 ซึ่งอาจเปิดโอกาสให้ผู้ไม่หวังดีสามารถสั่งรันคำสั่งบนเครื่องแม่ข่ายจากภายนอกได้โดยไม่ต้องยืนยันตัวตน ส่งผลให้ระบบสารสนเทศถูกควบคุม ข้อมูลรั่วไหลหรือถูกแก้ไขโดยไม่ได้รับอนุญาต รวมถึงระบบไม่สามารถให้บริการได้ และอาจถูกติดตั้งมัลแวร์เรียกค่าไถ่ นั้น

สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดชลบุรี ขอให้ท่านตรวจสอบเว็บไซต์และระบบงานสารสนเทศที่อยู่ในความรับผิดชอบ รวมถึงระบบที่มีผู้ให้บริการภายนอกเป็นผู้ดูแล พร้อมดำเนินการตามแนวทางการป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว ดังนี้ ๑. การสำรวจระบบและประเมินผลกระทบ ๒. การแก้ไขช่องโหว่ ๓. ป้องกันและจำกัดผลกระทบ ๔. การเฝ้าระวังความผิดปกติ ๕. การสำรองและกู้คืนข้อมูล

ทั้งนี้ ขอให้จัดทำแบบตอบรับการดำเนินการตามแนวทางการป้องกันและลดความเสี่ยงจากช่องโหว่ระดับวิกฤติใน PHP ตามสิ่งที่ส่งมาด้วย และจัดส่งทางไปรษณีย์อิเล็กทรอนิกส์ไปยัง cbi_nfedc@dole.go.th ภายในวันที่ ๙ พฤศจิกายน ๒๕๖๙ เพื่อรวบรวมและรายงานกรมส่งเสริมการเรียนรู้ภายในวันที่ ๑๐ พฤศจิกายน ๒๕๖๙ ต่อไป

จึงเรียนมาเพื่อทราบและดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ขอแสดงความนับถือ

(นางวิบูลผล พร้อมมูล)
ผู้อำนวยการสำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดชลบุรี

กลุ่มอำนวยการ
โทร ๐ ๓๘๒๘ ๗๑๔๘
ไปรษณีย์อิเล็กทรอนิกส์ : cbi_nfedc@dole.go.th

สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดชลบุรี
เลขที่รับ 4009
วันที่ 5 พ.ย. 2569
เวลา 11.09



**ด่วนที่สุด**
ที่ ศธ ๐๗๐๑๔/๔๗๙

ถึง ผู้อำนวยการสำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดทุกแห่ง / กรุงเทพมหานคร

ตามที่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ แจ้งกรณีพบช่องโหว่ระดับวิกฤตใน PHP หรือ PHP2Shell ได้แก่ CVE-2026-109618 และ CVE-2026-109619 ซึ่งอาจเปิดโอกาสให้ผู้ไม่หวังดีสามารถสั่งรันคำสั่งบนเครื่องแม่ข่ายจากภายนอกได้โดยไม่ต้องยืนยันตัวตน ส่งผลให้ระบบสารสนเทศถูกควบคุม ข้อมูลรั่วไหลหรือถูกแก้ไขโดยไม่ได้รับอนุญาต รวมถึงระบบไม่สามารถให้บริการได้ และอาจถูกติดตั้งมัลแวร์เรียกค่าไถ่ นั้น

กรมส่งเสริมการเรียนรู้ ขอให้ท่านตรวจสอบเว็บไซต์และระบบงานสารสนเทศที่อยู่ในความรับผิดชอบ รวมถึงระบบที่มีผู้ให้บริการภายนอกเป็นผู้ดูแล พร้อมดำเนินการตามแนวทางการป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว โดยสำรวจระบบที่ใช้งาน PHP ตรวจสอบเวอร์ชันที่ได้รับผลกระทบ และดำเนินการปรับปรุง PHP เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้ว หรือติดตั้งแพตช์ที่เกี่ยวข้อง ตลอดจนตรวจสอบมาตรการป้องกันระบบ การเฝ้าระวังความผิดปกติ การสำรอง และกู้คืนข้อมูล ทั้งนี้ ขอให้จัดทำแบบตรวจสอบและรายงานผลการแก้ไขช่องโหว่ตามเอกสารที่ส่งมาพร้อมนี้ และจัดส่งทางไปรษณีย์อิเล็กทรอนิกส์ไปยังกลุ่มเทคโนโลยีดิจิทัลและสารสนเทศ ภายในวันที่ ๑๐ พฤศจิกายน ๒๕๖๙ เพื่อรวบรวมและรายงานสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติต่อไป

จึงเรียนมาเพื่อดำเนินการในส่วนที่เกี่ยวข้องต่อไป




กลุ่มเทคโนโลยีดิจิทัลและสารสนเทศ
โทร. ๐ ๒๒๘๐ ๒๙๒๔
ไปรษณีย์อิเล็กทรอนิกส์ : dtech@dole.go.th

# ⚠ แจ้งเตือน

ด้านความปลอดภัยไซเบอร์ 22 ต.ค. 2569

# พบ 2 ช่องโหว่ PHP ระดับวิกฤต

## โจมตีจากระยะไกล · ไม่ต้องล็อกอิน · อัปเดตทันที

**CVE-2026-109618** Critical
หน่วยความจำเสียหาย (OOM)
ระดับความรุนแรง CVSS 9.2

**CVE-2026-109619** Critical
คำสถานะค้างข้ามคำขอ (UAF)
ระดับความรุนแรง CVSS 9.2



### ความเสี่ยงที่อาจเกิดขึ้น

ผู้โจมตีอาจสั่งรันโค้ดจากระยะไกล โดยไม่ต้องเข้าสู่ระบบ
ส่งผลให้ข้อมูลรั่วไหล ฝังเว็บเชลล์ หรือระบบถูกยึดควบคุม

## เวอร์ชัน PHP ที่ควรอัปเดต

| เวอร์ชันที่ใช้งาน | อัปเดตเป็น |
|---|---|
| PHP 8.5.11 หรือต่ำกว่าในสาขา 8.5 | 8.5.12 |
| PHP 8.4.26 หรือต่ำกว่าในสาขา 8.4 | 8.4.27 |
| PHP 8.3.35 หรือต่ำกว่าในสาขา 8.3 | 8.3.36 |
| PHP 8.2.34 หรือต่ำกว่าในสาขา 8.2 | 8.2.35 |

PHP 8.1 และต่ำกว่า สิ้นสุดการสนับสนุน ควรวางแผนย้ายไปใช้สาขาที่ยังได้รับการสนับสนุน

## แนวทางแก้ไขเร่งด่วน

**1 ตรวจรายการระบบ PHP** ทันที
เริ่มจากระบบที่เปิดสู่อินเทอร์เน็ต และ mod_php ใช้ `php -v`

**2 อัปเดต PHP แล้วรีสตาร์ต** ใน 24 ชม.
เป็น 8.2.35 8.3.36 8.4.27 8.5.12
มีคำสั่งแก้ที่ลบทุกเวอร์ชันเพียงวิธีเดียว

**3 แก้ทันทีไม่ได้? ลดความเสี่ยง** ชั่วคราว
- `session.upload_progress.enabled=0`
- PHP 8.5: `fatal_error_backtraces=0`
- ระบบเสี่ยงสูง: ตัดออกจากอินเทอร์เน็ต

**4 ตรวจร่องรอยการถูกเจาะ** หลังอัปเดต
ไฟล์ PHP แปลกใหม่ โพรเซสผิดปกติ
ล็อก POST ช่วง 20–22 ต.ค.

## หน่วยงานควรเร่งตรวจสอบและอัปเดตระบบ

หากพบเหตุผิดปกติ เก็บหลักฐานก่อนล้างระบบแล้วแจ้ง DG-CERT หรือ ThaiCERT

DGA | DG CERT

Shodan · PHP Security Advisories Team · watchTowr · Rapid7 · Tenable · Qualys · Censys · Wiz · GMO Cybersecurity by Ierae · Arctic Wolf · Google Cloud · Debian · Akamai · Fastly · Cloudflare · วันที่ 22 ต.ค. 2569

หน่วยงาน.....

# แบบตอบรับการดำเนินการตามแนวทางการป้องกันและลดความเสี่ยงจากช่องโหว่ระดับวิกฤติใน PHP

| ลำดับ | หัวข้อ | การตรวจสอบและการดำเนินการ | ผลการตรวจสอบ |
|---|---|---|---|
| 1 | การสำรวจระบบและประเมินผลกระทบ | หน่วยงานมีเว็บไซต์หรือระบบงานที่ใช้งาน PHP หรือไม่ โดยตรวจสอบจากหน้าจัดการเว็บไซต์หรือโฮสติ้ง หรือสอบถามผู้ดูแลระบบและผู้ให้บริการ | ☐ มี<br>☐ ไม่มี<br>☐ อยู่ระหว่างตรวจสอบ |
| | | มีระบบที่ใช้ PHP เวอร์ชันที่ได้รับผลกระทบ และยังไม่ได้รับการแก้ไขหรือไม่ โดยตรวจสอบเวอร์ชันที่ใช้งานจริงหรือให้ผู้ให้บริการยืนยันสถานะระบบ | ☐ มี<br>☐ ไม่มี<br>☐ อยู่ระหว่างตรวจสอบ |
| 2 | การแก้ไขช่องโหว่ | อัปเดต PHP เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้ว หรือติดตั้งแพตช์ที่เกี่ยวข้อง พร้อมตรวจสอบเวอร์ชัน | ☐ ดำเนินการแล้ว<br>☐ ยังไม่ดำเนินการ<br>☐ อยู่ระหว่างการตรวจสอบ |
| 3 | การป้องกันและจำกัดผลกระทบ | มี Firewall หรือ WAF ครอบคลุมระบบที่ใช้ PHP และเปิดใช้งานกฎที่เหมาะสม เพื่อจำกัดการเชื่อมต่อที่ไม่ได้รับอนุญาต หรือป้องกันการโจมตีเว็บไซต์ | ☐ มี<br>☐ ไม่มี |
| | | มีการแบ่งแยกเครือข่ายของเครื่องแม่ข่ายเว็บไซต์ออกจากระบบภายในที่สำคัญ และอนุญาตให้เชื่อมต่อได้เฉพาะที่จำเป็น เช่น ฐานข้อมูลที่ระบบต้องใช้งาน | ☐ มี<br>☐ ไม่มี<br>☐ อยู่ระหว่างตรวจสอบ |

หน่วยงาน.....

| ลำดับ | หัวข้อ | การตรวจสอบและการดำเนินการ | ผลการตรวจสอบ |
|---|---|---|---|
| 4 | การเฝ้าระวังและตรวจสอบความผิดปกติ | มีการเก็บบันทึกการเข้าใช้งานและข้อผิดพลาดของระบบ รวมถึงมีการตรวจสอบบันทึกเพื่อค้นหาความผิดปกติ | ☑ มี<br>☐ ไม่มี<br>☐ อยู่ระหว่างตรวจสอบ |
| 5 | การสำรองและกู้คืนข้อมูล | มีการสำรองไฟล์เว็บไซต์และฐานข้อมูลอย่างสม่ำเสมอ และมีการทดสอบว่าสามารถกู้คืนข้อมูลได้ | ☑ มี<br>☐ ไม่มี<br>☐ อยู่ระหว่างตรวจสอบ |

ลงชื่อ.....

(.....)

ตำแหน่ง.....

วันที่ ..... / ..... / .....

(หัวหน้าหน่วยงาน หรือผู้รับมอบอำนาจ)