



ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กพช. โทร. ๐ ๒๖๑๘ ๒๓๒๓ ต่อ ๑๐๑๒

ที่ นร. ๐๒๐๖.๐๓/ว๓๔๐

วันที่ ๖ พฤษภาคม ๒๕๖๕

เรื่อง แจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต

เรียน ผอ.สำนัก/กอง , ผอ.สปช.๑-๘ , ปชส. ๗๖ จังหวัด และหัวหน้าหน่วยงานสังกัด กปส.

ตามหนังสือ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ที่ สกมช. ๐๘๒๐/๒๖๓ ลงวันที่ ๑๙ เมษายน ๒๕๖๕ เรื่อง การแจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต นั้น

ในการนี้ ศสช. ขอให้หน่วยงานในสังกัด กปส.ที่มีการใช้งานระบบปฏิบัติการ Window ควรอัปเดตให้เป็นเวอร์ชันล่าสุด เพื่อความปลอดภัยและลดผลกระทบในการถูกโจมตีผ่านช่องโหว่ CVE-๒๐๒๒-๒๖๘๐๙ ดังนี้

๑. Block TCP port ๔๔๕ ที่ Firewall ขององค์กร เพื่อเป็นการลดการโจมตีผ่านช่องโหว่ CVE-๒๐๒๒-๒๖๘๐๙
๒. ปฏิบัติตามแนวทางของ Microsoft เพื่อรักษาความมั่นคงปลอดภัยการรับส่งข้อมูลของ SMB Protocol

จึงเรียนมาเพื่อโปรดทราบและดำเนินการต่อไป

(นางสาวอรุณญา เกตุแก้ว)

ผอ.ศสช.

กระดาษเขียนข่าว

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

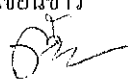
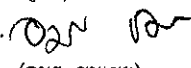
ศูนย์ข่าวคอมพิวเตอร์
 การประชาสัมพันธ์
 เลขรับ 35240
 วันที่ 6 พ.ค. 65
 เวลา 9.45

ความเร่งด่วนผู้รับปฏิบัติ	ลำดับความเร่งด่วน-ผู้รับทราบ	วัน เวลา	คำแนะนำในการส่งข่าว
ด่วนที่สุด	ด่วนที่สุด	เมษายน ๒๕๖๕	
จาก	ผู้อำนวยการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ		
ถึง	ผู้รับปฏิบัติ	ผู้ดูแลระบบ หรือผู้ที่เกี่ยวข้อง	ชั้นความลับ
	ผู้รับทราบ	หัวหน้าส่วนราชการ/หัวหน้าหน่วยงาน	ชื่อของผู้ให้ข่าว ที่ สกมช ๐๘๒๐/๒๖๓

๑. เพื่อกรุณาทราบ

๒. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ และได้ตรวจพบว่า มีช่องโหว่ระดับวิกฤต ที่ส่งผลกระทบต่อผู้ใช้งานระบบปฏิบัติการ Windows อย่างเป็นทางการ ที่ช่องโหว่ หมายเลข CVE-2022-26809 (Remote Procedure Call Runtime Remote Code Execution Vulnerability) เป็นช่องโหว่บนระบบปฏิบัติการ Windows ที่ผู้โจมตีสามารถเรียกใช้ remote code execution vulnerability in Remote Procedure Call Runtime Library ของระบบปฏิบัติการ Windows ซึ่งเป็นช่องโหว่ที่มีการเรียกใช้โค้ดจากระยะไกลในการเข้าถึงระบบปฏิบัติการ Windows โดยไม่ต้องผ่านการตรวจสอบสิทธิ์การเข้าถึงของระบบปฏิบัติการ ดังนั้นจึงขอให้ท่านตรวจสอบและดำเนินการป้องกันความเสียหายที่อาจเกิดขึ้นได้ ทั้งนี้ หากมีข้อสงสัยสามารถติดต่อสอบถามเพิ่มเติมได้ที่ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หมายเลขโทรศัพท์ ๐๘ ๐๓๓๙ ๙๓๗๘ หรือ E-mail : ncert@ncsa.or.th

หมายเหตุ รายละเอียดเพิ่มเติมปรากฏตามเอกสารแจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต

หน้า ๑ ของ ๑ หน้า	อ้างอิงข่าว	ผู้เขียนข่าว พ.ต.อ.  (ถัทภฤช พรหมจันทร์)	หน่วย ศปช.	โทรศัพท์ ๐๘ ๐๓๓๙ ๙๓๗๘
	ชั้นความลับ [] กำหนด [X] ไม่กำหนด			
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ			ผู้อนุมัติข่าว น.อ.  (อมร ชมเชย) รอง ผอ.สกมช.(๔)/ผอ.ศปช.	

เอกสารการแจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต
ตามกระดาษเขียนข่าวที่ สกมช 0820/๒๖๓ ลงวันที่ ๑๕ เมษายน 2565

Microsoft ได้เผยแพร่คำแนะนำเพื่อแก้ไขช่องโหว่ CVE-2022-26809
ผู้ใช้งานระบบปฏิบัติการ Windows ควรอัปเดตทันที

เมื่อวันที่ 13 เมษายน 2565 Cybersecurity and Infrastructure Security Agency (CISA) ได้ออกประกาศว่า Microsoft ได้เผยแพร่คำแนะนำเพื่อแก้ไขช่องโหว่ Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2022-26809)^[1] ซึ่งเป็นช่องโหว่ที่มีการเรียกใช้โค้ดจากระยะไกลในการเข้าถึงระบบปฏิบัติการ Windows โดยไม่ต้องผ่านการตรวจสอบสิทธิ์การเข้าถึงของระบบปฏิบัติการ

ช่องโหว่ Remote Procedure Call Runtime Remote Code Execution Vulnerability เป็นช่องโหว่บนระบบปฏิบัติการ Windows ที่ผู้โจมตีสามารถเรียกใช้ remote code execution vulnerability in Remote Procedure Call Runtime Library ของระบบปฏิบัติการ Windows สำหรับระบบปฏิบัติการที่ได้รับผลกระทบและการลดความเสี่ยงที่จะถูกโจมตีผ่านช่องโหว่นี้สามารถดูเพิ่มเติมได้ที่ <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809> หรือ scan QR Code



<https://bit.ly/3xAvHre>

หากองค์กรของท่านมีการใช้งานระบบปฏิบัติการ Windows ควรอัปเดตให้เป็นเวอร์ชันล่าสุด เพื่อความปลอดภัยและลดผลกระทบในการถูกโจมตี ทั้งนี้ Microsoft ได้มีคำแนะนำโดยทั่วไปในการลดความเสี่ยงที่จะถูกโจมตีผ่านช่องโหว่ CVE-2022-26809 ดังนี้

1. Block TCP port 445 ที่ Firewall ขององค์กร เพื่อเป็นการลดการโจมตีผ่านช่องโหว่ CVE-2022-26809 จากภายนอกองค์กร
2. ปฏิบัติตามแนวทางของ Microsoft เพื่อรักษาความมั่นคงปลอดภัยการรับส่งข้อมูลของ SMB Protocol^[2]

อ้างอิง

1. <https://www.cisa.gov/uscert/ncas/current-activity/2022/04/13/microsoft-releases-advisory-address-critical-remote-code-execution>
2. <https://docs.microsoft.com/th-th/windows-server/storage/file-server/smb-secure-traffic>