แจ้งเตือน : ช่องโหว่

ระดับ : Critical

ระดับ : High

ผลกระทบทางธุรกิจ

- ☒ Financial damage
- ☒ Reputation damage
- ☒ Non-compliance
- ☒ Privacy violation

ผลกระทบต่อระบบ

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

บริษัท Microsoft ออก Security Patch ประจำเดือนเมษายน 2565 เพื่อแก้ไขช่องโหว่ความสำคัญระดับ Critical และ High ควรติดตามและอัปเดต

วันที่แจ้งเตือน 20 เมษายน 2565

บริษัท Microsoft ผู้ผลิตและพัฒนาซอฟต์แวร์รายใหญ่ ได้ออกคำแนะนำเกี่ยวข้องกับ Security Patch จำนวน 145 รายการที่ส่งผลกระทบต่อผลิตภัณฑ์จำนวน 53 รายการ ประกอบด้วย Security Patch สำหรับแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรง และระดับสูง เช่น

ลำดับ	รายละเอียดช่องโหว่	หมายเลข CVE
1	ช่องโหว่บนบริการสั่งการทำงานจากระยะไกล (RPC Service) ที่เปิดโอกาสให้ผู้ไม่หวังดีเรียกใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution) ได้ ทั้งนี้ช่องโหว่ดังกล่าวยังมีผลกระทบต่อบริการเครือข่ายอื่น ๆ ที่มีการใช้ RPC Service เช่น SMB อีกด้วย	CVE-2022-26809
2	ช่องโหว่บริการแชร์ไฟล์ผ่านเครือข่าย (Network File System Service) ที่ผู้ไม่หวังดีใช้เทคนิคการปลอมแปลงข้อมูล (Crafted Message) โดยใช้โปรโตคอลข้างต้นส่งผลให้สามารถเรียกใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution)	CVE-2022-24491
3	ช่องโหว่ไดร์เวอร์ของระบบไฟล์สำหรับบันทึกเหตุการณ์ทั่วไป (Common Log File System Driver) ที่ทำให้ผู้ไม่หวังดีสามารถยกระดับสิทธิของระบบปฏิบัติการ (Local Privilege Escalation)	CVE-2022-24521

รายชื่อซอฟต์แวร์ที่ได้รับผลกระทบ เช่น ระบบปฏิบัติการ Windows และ Window Server โปรแกรม Microsoft Office เครื่องมือของซอฟต์แวร์การทำงานร่วมกัน (SharePoint) และโปรแกรมบราวเซอร์ Microsoft Edge เป็นต้น ทั้งนี้ สามารถตรวจสอบรายชื่อระบบปฏิบัติการและโปรแกรมที่ได้รับผลกระทบได้ที่ https://msrc.microsoft.com/update-guide

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบและพิจารณาดำเนินการอัปเดต Security Patch ของทางบริษัท Microsoft (Patch Tuesday) เพื่อแก้ไขช่องโหว่ของระบบปฏิบัติการและโปรแกรมที่ได้รับผลกระทบ
2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Security Patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

แจ้งเตือน : ช่องโหว่	ผลกระทบทางธุรกิจ	ผลกระทบต่อระบบ	TLP Color : White
ระดับ : Critical	☒ Financial damage ☒ Reputation damage ☒ Non-compliance ☒ Privacy violation	☒ Loss of Confidentiality ☒ Loss of Integrity ☒ Loss of Availability	 ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้
ระดับ : High			

บริษัท Microsoft ออก Security Patch ประจำเดือนเมษายน 2565 เพื่อแก้ไขช่องโหว่ความสำคัญระดับ Critical และ High ควรติดตามและอัปเดต

วันที่แจ้งเตือน 20 เมษายน 2565

ข้อมูลอ้างอิง

1. https://www.cisa.gov/uscert/ncas/current-activity/2022/04/12/microsoft-releases-april-2022-security-updates
2. https://blog.qualys.com/vulnerabilities-threat-research/2022/04/12/april-2022-patch-tuesday
3. https://cert.be/nl/microsoft-patch-tuesday-april-2022
4. https://www.techtarget.com/searchwindowsserver/news/252515900/Microsoft-plugs-Windows-zero-day-on-April-Patch-Tuesday
5. https://krebsonsecurity.com/2022/04/microsoft-patch-tuesday-april-2022-edition/
6. https://www.computerworld.com/article/3657754/aprils-patch-tuesday-a-lot-of-large-diverse-and-urgent-updates.html