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 ประจำเดือนมีนาคม 2565 เพื่อแก้ไขช่องโหว่ความสำคัญระดับร้ายแรงและระดับสูงควรติดตามและอัปเดต

วันที่แจ้งเตือน 9 มีนาคม 2565

บริษัท Microsoft ผู้ผลิตและพัฒนาซอฟต์แวร์รายใหญ่รายใหญ่ ได้ออกคำแนะนำเกี่ยวข้องกับ Security Patch จำนวน 71 รายการที่ส่งผลกระทบต่อผลิตภัณฑ์จำนวน 48 รายการ ประกอบด้วย Security Patch สำหรับแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรง และระดับสูง ได้แก่

ลำดับ	รายละเอียดช่องโหว่	หมายเลข CVE
1	ช่องโหว่บนเครื่องแม่ข่าย Microsoft Exchange Server ที่เปิดโอกาสให้ผู้ไม่หวังดีที่ได้รับสิทธิเข้าถึงระบบ (Authenticated User) สามารถโจมตีเพื่อส่งและเรียกใช้คำสั่งอันตรายจากระยะไกลโดยไม่ได้รับอนุญาต (Remote Arbitrary Code Execution)	CVE-2022-23277
2	ช่องโหว่บนโปรแกรมสำหรับใช้เชื่อมต่อโดยใช้ Remote Desktop Protocol (RDP Client) ที่เปิดโอกาสให้ผู้ไม่หวังดีสามารถอ่านหน่วยความจำ Heap (Heap Memory) ในส่วนที่ไม่เกี่ยวข้องก่อให้เกิดความเสี่ยงด้านข้อมูลรั่วไหล	CVE-2022-24503
3	ช่องโหว่ของโปรโตคอลการรับส่งไฟล์บนระบบเครือข่ายเวอร์ชัน 3 (Server Message Block Version 3) ที่เปิดโอกาสให้ผู้ที่ไม่หวังดีที่ได้รับสิทธิเข้าถึงระบบ (Authenticated User) สามารถส่งและเรียกใช้คำสั่งจากระยะไกลโดยไม่ได้รับอนุญาตโดยมีผลกระทบทั้งซอฟต์แวร์เครื่องลูกข่าย (Client) และเครื่องแม่ข่าย (Server)	CVE-2022-24508

รายชื่อซอฟต์แวร์ที่ได้รับผลกระทบ เช่น ระบบปฏิบัติการ Windows และ Window Server โปรแกรม Microsoft Office และเครื่องแม่ข่ายสำหรับการรับส่ง e-mail (Microsoft Exchange Server) ระบบบริหารจัดการเครื่องแม่ข่ายเสมือน (Hyper-V) เป็นต้น ทั้งนี้ สามารถตรวจสอบรายชื่อระบบปฏิบัติการและโปรแกรมที่ได้รับผลกระทบได้ที่ https://msrc.microsoft.com/update-guide

<u>เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการ ดังนี้</u>

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

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

บริษัท Microsoft ออก Security Patch ประจำเดือนมีนาคม 2565 เพื่อแก้ไขช่องโหว่ความสำคัญระดับร้ายแรงและระดับสูงควรติดตามและอัปเดต

วันที่แจ้งเตือน 9 มีนาคม 2565

ข้อมูลอ้างอิง

1. https://us-cert.cisa.gov/ncas/current-activity/2022/03/08/microsoft-releases-march-2022-security-updates
2. https://auscert.org.au/bulletins/?cat_id=21
3. https://www.rapid7.com/blog/post/2022/03/08/patch-tuesday-march-2022/
4. https://www.zdnet.com/article/microsoft-march-2022-patch-tuesday-71-vulnerabilities-fixed/
5. https://www.helpnetsecurity.com/2022/03/08/march-2022-patch-tuesday/