แจ้งเตือน : ช่องโหว่

ระดับ : Critical

ระดับ : High

ผลกระทบทางธุรกิจ

- [x] Financial damage
- [x] Reputation damage
- [x] Non-compliance
- [ ] Privacy violation

ผลกระทบต่อระบบ

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

บริษัท Microsoft ออก Security Patch ประจำเดือนมกราคม 2565 แก้ไขช่องโหว่ระดับ Critical และ High ควรติดตามและอัปเดต

วันที่แจ้งเตือน 14 มกราคม 2565

บริษัท Microsoft ผู้ผลิตและพัฒนาซอฟต์แวร์รายใหญ่รายใหญ่ ได้ออกคำแนะนำเกี่ยวข้องกับ Security Patch จำนวน 97 รายการที่ส่งผลกระทบต่อผลิตภัณฑ์จำนวน 64 รายการ ประกอบด้วย Security Patch สำหรับแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรงและสูง เช่น

ลำดับ	รายละเอียดช่องโหว่	หมายเลข CVE
1	ช่องโหว่ในไลบรารีที่ใช้ประมวลผล HTTP Protocol Stack ส่งผลให้ผู้ไม่หวังดีสามารถเรียกใช้ช่องโหว่การใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution)	CVE-2022-21907
2	ช่องโหว่ที่ใช้เทคนิคการปลอมแปลงเอกสารแนบ (Crafted File) ส่งผลให้สามารถเรียกใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution)	CVE-2022-21840
3	ช่องโหว่ที่ถูกใช้เพื่อการยกระดับสิทธิของระบบปฏิบัติการ (Local Privilege Escalation) บนเครื่องแม่ข่ายสำหรับบริการยืนยันพิสูจน์ตัวตนผู้ใช้งาน (Active Directory Domain Services)	CVE-2022-21857
4	ช่องโหว่ที่ถูกใช้เพื่อการยกระดับสิทธิของระบบปฏิบัติการ(Local Privilege Escalation) บนเครื่องมือเชื่อมต่อระบบงานภายในของระบบบริหารจัดการเครื่องแม่ข่ายเสมือน (Integrated Drive Electronics)	CVE-2022-21833

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

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

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

แจ้งเตือน : ช่องโหว่

ระดับ : Critical

ระดับ : High

ผลกระทบทางธุรกิจ

- [x] Financial damage
- [x] Reputation damage
- [x] Non-compliance
- [ ] Privacy violation

ผลกระทบต่อระบบ

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

บริษัท Microsoft ออก Security Patch ประจำเดือนมกราคม 2565 แก้ไขช่องโหว่ระดับ Critical และ High ควรติดตามและอัปเดต

วันที่แจ้งเตือน 14 มกราคม 2565

ข้อมูลอ้างอิง

1. https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/microsoft-releases-january-2022-security-updates
2. https://www.auscert.org.au/bulletins/ASB-2022.0006
3. https://www.bleepingcomputer.com/news/microsoft/microsoft-january-2022-patch-tuesday-fixes-6-zero-days-97-flaws/
4. https://www.zdnet.com/article/malsmoke-hackers-now-abuse-microsoft-e-signature-verification-tool-in-cyberattacks/