แจ้งเตือน : ช่องโหว่

ผลกระทบ : High

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [ ] Non-compliance
- [ ] Privacy Violation

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ประเภท RCE ผ่านการใช้งานโปรแกรม MS Word (CVE-2022-30190 หรือ Follina)

วันที่แจ้งเตือน 21 มิถุนายน 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับช่องโหว่ประเภท RCE (Remote Code Execution) จากการใช้งานโปรแกรม MS Word (CVE 2022-30190) ซึ่งทำให้ผู้ไม่หวังดีอาศัยช่องโหว่นี้ โดยการฝัง URL ในเอกสาร ตามรูปแบบ ms-msdt:/(Microsoft Support Diagnostic Tool) เพื่อเข้าควบคุมระบบและโปรโตคอลได้จากระยะไกล และส่งอีเมลพร้อมแนบไฟล์ MS Word หลอกเหยื่อ โดยเมื่อผู้ใช้เปิดเอกสารแล้ว Code ที่เป็นอันตรายจะทำงานทันที ไม่ว่าจะเป็นการเปิดเอกสารในรูปแบบพรีวิว เปิดแบบ Read-only หรือเปิดใน MS Word ที่ปิดการใช้งานมาโคร ซึ่งผู้ไม่หวังดีจะสามารถติดตั้งโปรแกรมเพื่อเปลี่ยนแปลงข้อมูล ลบข้อมูล สร้างบัญชีใหม่ หรือขโมยข้อมูลส่วนตัวได้

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ใช้งานและผู้ดูแลระบบ ควรพิจารณาดำเนินการ ดังนี้

1) ควรเพิ่มการตรวจสอบ หรือ เพิ่มความระมัดระวังในการเปิดไฟล์ MS Word ที่ได้รับจากผู้ส่งที่ไม่รู้จัก
2) ติดตั้ง Patch ตามที่ Microsoft ประกาศ โดยผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง (อ่านรายละเอียดได้ที่ข้อมูลอ้างอิง 1)
3) ปิดการใช้งานโปรโตคอล MSDT URL เพื่อป้องกันไม่ให้ตัวแก้ไขปัญหา (Diagnostic Tools) เปิดใช้งานลิงก์จากผู้ไม่หวังดี (ตรวจสอบวิธีการได้จากข้อมูลอ้างอิง 2)
4) หมั่น update โปรแกรม Antivirus ให้เป็นปัจจุบันอยู่เสมอ กรณีที่มีการใช้งาน Microsoft Defender Antivirus (MDAV) ให้พิจารณาใช้งาน signatures detection build 1.367.851.0 หรือ สูงกว่า และเปิดใช้ cloud-delivered protection และ automatic sample submission
5) หากมีการใช้งาน Microsoft Defender for Endpoint (MDE) เพื่อช่วยในการตรวจจับและแจ้งเตือน ให้เลือกหัวข้อการตรวจจับใน Microsoft 365 Defender portal เป็น Suspicious behavior by an Office application และ Suspicious behavior by Msdt.exe

ข้อมูลอ้างอิง

1) https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190
2) https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/
3) https://mgronline.com/cyberbiz/detail/9650000057966?fbclid=IwAR0C3L-uTUnHPNAsqt_zHC5Rg4HAuzneJqM-JnHo_o1ITaGBp1e2CAP0zWI
4) https://nvd.nist.gov/vuln/detail/CVE-2022-30190