ด่วนที่สุด บันทึกข้อความ

ส่วนราชการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ กลุ่มอำนวยการ โทร. ๐ ๒๕๙๐ ๔๓๑๐

ที่ สธ ๐๙๔๙.๐๑/ว ๑๖๗ **วันที่** ๑๕ มีนาคม ๒๕๖๗

เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๘/๖๗

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ ผู้อำนวยการสำนักทุกสำนัก ผู้อำนวยการกองทุกกอง ผู้อำนวยการศูนย์ทุกศูนย์ ผู้อำนวยการกลุ่มทุกกลุ่ม ผู้อำนวยการสถาบันทุกสถาบัน เลขานุการกรม

ตามที่ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ได้รับมอบหมายให้มีการติดตาม เฝ้าระวังภัยคุกคามทางไซเบอร์ และเป็นศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์กรมอนามัย เพื่อเตรียมพร้อมรับมือ แก้ไขและป้องกันเหตุการณ์ภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานภายใต้สังกัดกรมอนามัย นั้น

ในการนี้ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ขอแจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ กรณี Microsoft Patch Tuesday เดือนมีนาคม ๒๐๒๔ ได้แก้ไขช่องโหว่จำนวน ๕๙ รายการ ทั้งนี้ ให้ท่านดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานที่อาจเกี่ยวข้องกับเหตุการณ์ดังกล่าว เพื่อเป็นการยกระดับการเฝ้าระวังและป้องกันการโจมตี และลดความเสี่ยงที่อาจจะเกิดขึ้น รายละเอียดตามเอกสารแนบ หากมีข้อสงสัยสามารถสอบถามได้ที่ นายภัทร์รพี สีบุตตะ หมายเลขโทรศัพท์ ๐ ๒๕๙๐ ๔๓๑๐

จึงเรียนมาเพื่อโปรดทราบ

มอบHR ทราบ/ดำเนินการ
(นางศิริพรรณ บุตรศรี)
(ลายเซ็นต์อิเล็กทรอนิกส์)
นักวิชาการสาธารณสุขเชี่ยวชาญ (ด้านโภชนาการ)
รักษาราชการแทนผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง
18 มีนาคม 2567

(นางสาวชุลีวรรณ นพวิสุทธิสกุล)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ปฏิบัติหน้าที่ผู้อำนวยการกองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย

(นางสาวเกศรา โชคนำชัยสิริ)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

กรม
๒๔ มี.ค. 67

ThaiCERT Infoshare

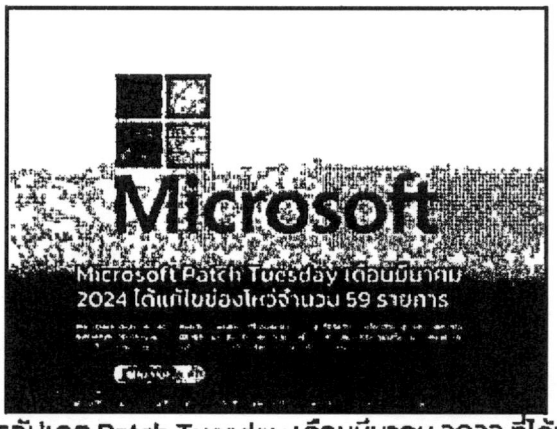
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

ประจำวันพฤหัสบดีที่ 14 มีนาคม 2567

NCSA สกมช

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Microsoft Patch Tuesday เดือนมีนาคม 2024 ได้แก้ไขช่องโหว่จำนวน 59 รายการ



Microsoft ออกการอัปเดต Patch Tuesday เดือนมีนาคม 2023 ที่ได้แก้ไขช่องโหว่จำนวน 59 รายการในผลิตภัณฑ์ โดยมีช่องโหว่ 2 รายการที่ CVE-2024-21407 และ CVE-2024-21408 ถูกจัดอันดับเป็น Critical และอีก 57 รายการที่เหลือได้รับการจัดอันดับเป็น Important ตามระดับความรุนแรง

- ช่องโหว่ CVE-2024-21407 เป็นช่องโหว่ Remote Code Execution ใน Windows Hyper-V
- ช่องโหว่ CVE-2024-21408 เป็นช่องโหว่ Denial of Service ใน Windows Hyper-V

ช่องโหว่ที่รุนแรงที่สุดที่ได้รับการแก้ไขโดย Microsoft คือช่องโหว่ Open Management Infrastructure (OMI) ที่สามารถ Remote Code Execution ที่ CVE-2024-21334 (CVSS 9.8) โดย Attacker ที่ไม่ได้รับการรับรองความถูกต้องสามารถ execute code บน OMI instances โดยสามารถเข้าถึงได้ผ่านทาง Internet

โดยในขณะนี้ยังไม่มีช่องโหว่ใดที่ได้รับแก้ไขจากการอัปเดตความปลอดภัย Microsoft Patch Tuesday เดือนมีนาคม 2023 ที่มีการถูกนำไปใช้ในการโจมตี โดยรายการช่องโหว่ทั้งหมดที่ Microsoft แก้ไขในเดือนมีนาคม 2024 โดยสามารถดูเพิ่มเติมได้ที่ https://www.zerodayinitiative.com/blog/2024/3/12/the-march-2024-security-update-review

ที่มาของข่าว - https://securityaffairs.com/160412/security/microsoft-patch-tuesday-march-2024.html