ระวังภัย ช่องโหว่ใน Microsoft Windows DNS ผู้ไม่หวังดีสามารถสั่งรันโค้ดอันตรายควบคุมเครื่องให้บริการได้ (CVE-2015-6125, MS15-127)

วันที่ประกาศ: 9 ธันวาคม 2558
ปรับปรุงล่าสุด: 9 ธันวาคม 2558
เรื่อง: ระวังภัย ช่องโหว่ใน Microsoft Windows DNS ผู้ไม่หวังดีสามารถสั่งรันโค้ดอันตรายควบคุมเครื่องให้บริการได้ (CVE-2015-6125, MS15-127)
ประเภทภัยคุกคาม: Intrusion

ข้อมูลทั่วไป

เมื่อวันที่ 8 ธันวาคม 2558 บริษัทไมโครซอฟท์ออกบทความแจ้งเตือนช่องโหว่ของบริการ Microsoft Windows DNS โดยมีข้อมูลสำคัญว่าผู้ไม่ประสงค์ดีสามารถส่งคำสั่งอันตรายไปยังบริการดังกล่าว และสามารถสั่งรันโค้ดอันตรายบนเครื่องให้บริการนั้นได้ทันที (เป็นการโจมตีประเภท Remote Code Execution) โดยมีการจำแนกระดับความรุนแรงของช่องโหว่ดังกล่าวเป็น Critical ซึ่งหมายถึงระดับความรุนแรงสูงสุด

ปัจจุบันยังไม่พบการเผยแพร่โค้ดตัวอย่างหรือวิธีที่ใช้ในการโจมตีช่องโหว่ดังกล่าว โดยอาจประเมินได้ว่าอาจมีการเผยแพร่วิธีการโจมตีในอนาคตอันใกล้ หรือในอีกมุมหนึ่งหมายถึงปัจจุบันช่องโหว่ดังกล่าวถูกใช้โจมตีบริการทั่วโลกอยู่ ณ ขณะนี้

ผลกระทบ

ผู้ไม่ประสงค์ดีสามารถสั่งให้โค้ดอันตรายทำงานและเข้าควบคุมระบบหรือเครื่องของเหยื่อที่มีช่องโหว่ได้จากระยะไกล (Remote Code Execution)

ระบบที่ได้รับผลกระทบ

- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2012
- Windows Server 2012 R2

ข้อแนะนำในการป้องกันและแก้ไข

Microsoft ได้ออกซอฟต์แวร์อัปเดตเพื่อแก้ไขช่องโหว่นี้แล้ว ผู้ใช้งาน สามารถอัปเดตอัตโนมัติจากซอฟต์แวร์ Windows Update หรือดาวน์โหลด [1] โดยเลือกติดตั้งอัปเดตตามเวอร์ชันที่ใช้งาน

อ้างอิง

1. https://technet.microsoft.com/en-us/library/security/ms15-127.aspx