

- Financial Damage
- Reputation Damage
- Non-compliance
- Privacy Violation

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability



แจ้งเตือนเพื่อ Update Apple Patch (CVE-2022-42827) แก้ไขช่องโหว่ Zero-day

วันที่แจ้งเตือน 27 ตุลาคม 2565

เมื่อวันที่ 24 ตุลาคม 2565 บริษัท Apple ได้ออกชุดอัปเดตฉุกเฉินเพื่อแก้ไขช่องโหว่หรือจุดบกพร่องของซอฟต์แวร์ (Patch) สำหรับช่องโหว่ Zero-Day หมายเลข CVE-2022-42827 (Kernel) ซึ่งเป็นช่องโหว่ที่เกิดจากการที่ซอฟต์แวร์สามารถเขียนข้อมูลนอกขอบเขตของบัฟเฟอร์หน่วยความจำ (Out-of-Bound Write) ส่งผลให้แอปพลิเคชันอาจสามารถรันโค้ดโดยพลการได้ด้วยสิทธิ์ของ Kernel ซึ่งบริษัท Apple ยืนยันว่ามีการใช้ประโยชน์จากช่องโหว่ดังกล่าวแล้ว

อุปกรณ์ที่ได้รับผลกระทบได้แก่ iPhone 8 หรือสูงกว่า, iPad Pro (ทุกโมเดล), iPad Air 3rd generation หรือสูงกว่า, iPad 5th generation หรือสูงกว่า และ iPad mini 5th generation หรือสูงกว่า

ทั้งนี้ บริษัท Apple ได้ออก Patch เพื่อแก้ไขช่องโหว่ดังกล่าว ซึ่งจะถูอัปเดตโดยอัตโนมัติจาก Apple (หากมีการตั้งค่าเป็น Automatic updates) เป็นเวอร์ชันใหม่ ได้แก่ iOS 16.1 และ iPadOS 16

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น บริษัทควรแนะนำให้บุคลากรภายในองค์กรดำเนินการติดตั้ง Patch ตามที่ บริษัท Apple แนะนำ กับอุปกรณ์ส่วนตัวและอุปกรณ์ของบริษัท สำหรับแม่ข่าย ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนดำเนินการ

ข้อมูลอ้างอิง

- 1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันพุธที่ 26 ตุลาคม 2565
- 2) <https://www.bleepingcomputer.com/news/apple/apple-fixes-new-zero-day-used-in-attacks-against-iphones-ipads/>
- 3) <https://thehackernews.com/2022/10/apple-releases-patch-for-new-actively.html>
- 4) <https://support.apple.com/en-us/HT213489#:~:text=improved%20bounds%20checking.-,CVE%2D2022%2D42827,-%3A%20an%20anonymous%20researcher>