แจ้งเตือน : ช่องโหว่

HIGH

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนเพื่อ Update Google Patch (CVE-2022-2856) และ Apple Patch (CVE-2022-32894 และ CVE-2022-32893) แก้ไขช่องโหว่ Zero-day

วันที่แจ้งเตือน 19 สิงหาคม 2565

เมื่อวันที่ 16 สิงหาคม 2565 Google ได้ออกชุดอัปเดตเพื่อแก้ไขช่องโหว่หรือจุดบกพร่องในซอฟต์แวร์ (Patch) สำหรับ Chrome Browser บน Desktop เพื่อแก้ไขช่องโหว่ Zero-Day ที่มีความรุนแรงสูงสามารถนำไปใช้ในการโจมตีได้

ช่องโหว่หมายเลข CVE-2022-2856 เกิดจากการตรวจสอบข้อมูลนำเข้า (untrusted input) ที่ไม่เพียงพอใน Web Intents (อ้างอิง 4) โดยชุดอัปเดตล่าสุดยังครอบคลุมถึงช่องโหว่ด้านความปลอดภัยอื่น ๆ อีก 10 รายการ ซึ่งส่วนใหญ่เกี่ยวข้องกับช่องโหว่ประเภท Use-After-Free (UAF) ซึ่งส่งผลทำให้ข้อมูลเสียหายหรือโปรแกรมขัดข้องได้ (อ้างอิง 5) เช่น FedCM, SwiftShader, ANGLE และ Blink รวมถึงช่องโหว่ Heap buffer overflow เป็นต้น

ผู้ใช้งานควรอัปเดต เป็นเวอร์ชัน 104.0.5112.101 สำหรับ macOS และ Linux, เวอร์ชัน 104.0.5112.102/101 สำหรับ Windows เพื่อลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้น ผู้ใช้งาน Browserที่ใช้ Chromium เช่น Microsoft Edge, Brave, Opera และ Vivaldi ควรอัปเดตเป็นเวอร์ชันใหม่ให้เร็วที่สุด

นอกจากนั้น ในวันที่ 17 สิงหาคม 2565 Apple ได้ออก Patch ฉุกเฉินสำหรับช่องโหว่ Zero-Day ในแพลตฟอร์ม macOS และ iOS โดย Apple ยืนยันว่ามีการใช้ประโยชน์จากช่องโหว่ดังกล่าว โดยเป็นช่องโหว่ที่เกิดจากข้อบกพร่องในการรันโค้ด (Code execution) ซึ่งตรวจพบใน อุปกรณ์ iPhone, iPad และ macOS ดังนี้

ช่องโหว่หมายเลข CVE-2022-32894 (Kernel) ส่งผลให้แอปพลิเคชันอาจสามารถรันโค้ดด้วยสิทธิของ Kernel ช่องโหว่หมายเลข CVE-2022-32893 (WebKit) เกี่ยวกับการประมวลผลเนื้อหาเว็บที่ออกแบบมาโดยมีจุดประสงค์ที่ไม่หวังดี ส่งผลให้อาจทำให้มีการรันโค้ดโดยพลการได้ ทั้งนี้ Patch จะถูกอัปเดตโดยอัตโนมัติจาก Apple (หากมีการตั้งค่าเป็น Automatic updates) เป็นเวอร์ชันใหม่ ดังนี้ macOS Monterey 12.5.1, iOS 15.6.1 และ iPadOS 15.6.1

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น บริษัทควรแนะนำให้บุคลากรภายในองค์กรดำเนินการติดตั้ง Patch ตามที่ Google และ Apple แนะนำ ทั้งกับอุปกรณ์ส่วนตัวและอุปกรณ์ของบริษัท สำหรับเครื่องแม่ข่าย (Server) ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนดำเนินการ

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันศุกร์ที่ 19 สิงหาคม 2565
2) https://thehackernews.com/2022/08/new-google-chrome-zero-day.html
3) https://chromereleases.googleblog.com/2022/08/stable-channel-update-for-desktop_16.html
4) https://www.chromium.org/developers/web-intents-in-chrome/
5) https://encyclopedia.kaspersky.com/glossary/use-after-free/
6) https://www.securityweek.com/apple-patches-new-macos-ios-zero-days