

วันที่ 5 ตุลาคม 2569

ช่องโหว่ Zero-Day ใน FortiMail ถูกโจมตีแล้ว เปิดช่องให้ผู้โจมตีเขียนไฟล์ใดๆ ในระบบได้โดยไม่ต้องยืนยันตัวตน



สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) เมื่อวันพฤหัสบดีที่ผ่านมา ได้เพิ่มช่องโหว่ด้านความปลอดภัยระดับวิกฤตที่ส่งผลกระทบต่ Fortinet FortiMail ลงในรายการ Known Exploited Vulnerabilities (KEV) หลังพบรายงานว่าช่องโหว่ดังกล่าวกำลังถูกนำไปใช้โจมตีจริง ช่องโหว่นี้ถูกติดตามในชื่อ CVE-2026-104286 (คะแนน CVSS: 9.8) เปิดโอกาสให้ผู้โจมตีที่ไม่ต้องเข้าสู่ระบบ สามารถเขียนไฟล์ใดๆ ลงบนระบบที่อยู่เบื้องหลังได้

Fortinet ระบุในคำแนะนำด้านความปลอดภัยว่า ช่องโหว่นี้เกิดจากการตรวจสอบเส้นทางไฟล์ที่ไม่รัดกุม ซึ่งทำให้สามารถเข้าถึงไฟล์เดอร์ที่ไม่ควรเข้าถึงได้ (Path Traversal) รวมถึงการจัดการค่า NULL Byte หรืออักขระ NULL ที่ไม่เหมาะสม (CWE-158) โดยผู้โจมตีที่ไม่ต้องยืนยันตัวตนสามารถส่งคำขอ HTTP หรือ HTTPS ที่สร้างขึ้นเป็นพิเศษ เพื่อเขียนไฟล์ใดๆ ลงบนระบบได้

ช่องโหว่นี้ส่งผลกระทบต่อเวอร์ชันต่อไปนี้

- FortiMail 8.0.0 ถึง 8.0.1 (ให้อัปเกรดเป็นเวอร์ชัน 8.0.2 หรือใหม่กว่าเมื่อมีการเปิดตัว)
- FortiMail 7.6.0 ถึง 7.6.6 (ให้อัปเกรดเป็นเวอร์ชัน 7.6.7 หรือใหม่กว่าเมื่อมีการเปิดตัว)
- FortiMail 7.4.0 ถึง 7.4.8 (ให้อัปเกรดเป็นเวอร์ชัน 7.4.9 หรือใหม่กว่าเมื่อมีการเปิดตัว)
- FortiMail 7.2.0 ถึง 7.2.9 (ให้อัปเกรดไปใช้สายเวอร์ชัน 7.4 หรือใหม่กว่า)

Fortinet ยืนยันแล้วว่าช่องโหว่นี้ถูกนำไปใช้โจมตีจริง และแนะนำให้ลูกค้าดำเนินการตามแนวทางชั่วคราวต่อไปนี้จนกว่าจะมีการออกแพตช์สำหรับบางเวอร์ชัน

ปิดการใช้งานฟีเจอร์ IBE Support โดยใช้คำสั่ง CLI ต่อไปนี้

```
config system encryption ibe  
set status disable  
end
```

ปิดการเข้าถึงหน้าจัดการ FortiMail จากอินเทอร์เน็ต หรือจำกัดการเข้าถึงให้สามารถใช้งานได้เฉพาะจากเครือข่ายภายในที่เชื่อถือได้เท่านั้น โดย Fortinet ระบุว่า Gwendal Guégnaud จากทีม Fortinet Product Security เป็นผู้ค้นพบและรายงานช่องโหว่นี้ พร้อมเปิดเผยข้อมูลที่สามารถใช้ตรวจสอบการบุกรุก (Indicators of Compromise: IoC) ดังต่อไปนี้

ที่อยู่ IP

- 79.141.169[.]187
- 45.129.0[.]192

ไฟล์

- /data/lib/liblog.so (ถูกเพิ่มเข้ามา)
- /data/bin/webconsole (ถูกเพิ่มเข้ามา)
- /data/bin/mailservice (ถูกเพิ่มเข้ามา)
- /data/etc/ld.so.preload (ถูกเพิ่มเข้ามา)
- /bin/smit (ถูกแก้ไข)
- /data/etc/httpd.conf (ถูกแก้ไข)
- /data/migadmin.tar.gz (ถูกแก้ไข)

เนื่องจากพบการนำช่องโหว่นี้ไปใช้โจมตีจริง หน่วยงานภาครัฐของสหรัฐฯ ในกลุ่ม Federal Civilian Executive Branch (FCEB) จึงได้รับคำแนะนำให้ติดตั้งแพตช์หรือใช้แนวทางป้องกันชั่วคราวภายในวันที่ 4 ตุลาคม 2026

เหตุการณ์ดังกล่าวเกิดขึ้นในช่วงเวลาเดียวกับที่ช่องโหว่ด้านความปลอดภัยหลายรายการในผลิตภัณฑ์ของ Check Point (CVE-2026-85102 และ CVE-2026-93616), Arista VeloCloud Orchestrator (CVE-2026-93952), F5 BIG-IP Access Policy Manager (CVE-2026-94127), Cisco Catalyst SD-WAN Manager (CVE-2026-76504) และ Citrix NetScaler ADC และ NetScaler Gateway (CVE-2026-88771 และ CVE-2026-88772) ก็ถูกนำไปใช้โจมตีจริงเช่นกัน

ข้อมูลอ้างอิง

Oct 2, 2026, By Ravie Lakshmanan

- <https://thehackernews.com/2026/10/critical-fortimail-zero-day-flaw.html>