บันทึกข้อความ

ส่วนราชการ กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน โทร. ๐ ๒๕๒๑ ๖๕๕๐ ต่อ ๓๐๓

ที่ สธ ๐๙๓๕.๐๒/ ว ๑๕๗ **วันที่** ๒๒ กุมภาพันธ์ ๒๕๖๗

เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๓/๖๗

เรียน รองผู้อำนวยการฯ / หัวหน้ากลุ่มงาน

ตามหนังสือกลุ่มอำนวยการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ที่ สธ ๐๙๔๙.๐๑/ว๑๕๔ ลงวันที่ ๑๙ กุมภาพันธ์ ๒๕๖๗ เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๓/๖๗ จากกรณี ตรวจพบช่องโหว่ในการเรียกใช้งานโค้ดระยะไกล หรือ Remote Code Execution (RCE) ใหม่ใน Fortinet SSL VPN และช่องโหว่ใน FortiSIEM โดยให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของหน่วยงานที่อาจเกี่ยวข้องกับเหตุการณ์ดังกล่าว ความละเอียดแจ้งแล้วนั้น

ในการนี้ กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน จึงขอประชาสัมพันธ์และสื่อสารให้ท่านและบุคลากรในกลุ่มงานทุกท่าน ทราบถึงแนวทางการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ รายละเอียดตาม QR Code ที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อทราบและแจ้งบุคลากรในกลุ่มงานของท่านทราบและถือปฏิบัติอย่างเคร่งครัดต่อไปด้วย จะเป็นพระคุณ

(นายนิธิรัตน์ บุญตานนท์)
ผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง

งานพัฒนาองค์กรและขับเคลื่อนกำลังคน
รับวันที่ 20 ก.พ. 67
เวลา 9.47 น.
เลขที่รับ 229

บันทึกข้อความ

ส่วนราชการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ กลุ่มอำนวยการ โทร. ๐ ๒๕๙๐ ๔๓๑๐
ที่ สธ ๐๙๔๙.๐๑/๑๒๕๔ **วันที่** ๑๙ กุมภาพันธ์ ๒๕๖๗
เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๓/๖๗

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ ผู้อำนวยการสำนักทุกสำนัก ผู้อำนวยการกองทุกกอง ผู้อำนวยการศูนย์ทุกศูนย์ ผู้อำนวยการกลุ่มทุกกลุ่ม ผู้อำนวยการสถาบันทุกสถาบัน เลขานุการกรม

ตามที่ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ได้รับมอบหมายให้มีการติดตาม เฝ้าระวังภัยคุกคามทางไซเบอร์ และเป็นศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์กรมอนามัย เพื่อเตรียมพร้อมรับมือ แก้ไขและป้องกันเหตุการณ์ภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานภายใต้สังกัดกรมอนามัย นั้น

ในการนี้ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ขอแจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ จากกรณีตรวจพบช่องโหว่ในการเรียกใช้โค้ดระยะไกล หรือ Remote Code Execution(RCE) ใหม่ใน Fortinet SSL VPN และช่องโหว่ใน FortiSIEM ทั้งนี้ ให้ท่านดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานที่อาจเกี่ยวข้องกับเหตุการณ์ดังกล่าว เพื่อเป็นการยกระดับการเฝ้าระวังและป้องกันการโจมตี รายละเอียดตามเอกสารแนบ หากมีข้อสงสัยสามารถสอบถามได้ที่ นายภัทร์รพี สีบุตตะ หมายเลขโทรศัพท์ ๐ ๒๕๙๐ ๔๓๑๐

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการต่อไป จะเป็นพระคุณ

(นางสาวชุลีวรรณ นพวิสุทธิสกุล)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ปฏิบัติหน้าที่ผู้อำนวยการกองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย

ทราบ/ดำเนินการ
(นางสาวเกศรา โชคนำชัยสิริ)
(ลายเซ็นต์อิเล็กทรอนิกส์)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
รองผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง
19 กุมภาพันธ์ 2567

มอบ HR
(นายนิธิรัตน์ บุญตานนท์)
ผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง
19 กุมภาพันธ์ 2567

ทราบ
22 ก.พ. 67

(นางสาวเกศรา โชคนำชัยสิริ)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

HealthCERT

12 กุมภาพันธ์ 2567

TLP CLEAR

แจ้งเตือน (ฉบับแก้ไข) ช่องโหว่การเรียกใช้โค้ดระยะไกล หรือ Remote Code Execution(RCE) ใหม่ ใน Fortinet SSL VPN

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ออกประกาศแจ้งเตือนกรณีพบช่องโหว่การเรียกใช้โค้ดระยะไกล หรือ RCE ใหม่ใน Fortinet SSL VPN หมายเลขช่องโหว่ CVE-2024-21762 ความรุนแรงระดับ Critical (คะแนน CVSS : 9.6) ซึ่งเป็นช่องโหว่ Out-of bounds wite ใน FortiOS ทำให้ผู้โจมตีที่ไม่ได้รับอนุญาต สามารถเรียกใช้โค้ดจากระยะไกล

Version	Affected	Solution
FortiOS 7.6	Not affected	Not Applicable
FortiOS 7.4	7.4.0 through 7.4.2	Upgrade to 7.4.3 or above
FortiOS 7.2	7.2.0 through 7.2.6	Upgrade to 7.2.7 or above
FortiOS 7.0	7.0.0 through 7.0.13	Upgrade to 7.0.14 or above
FortiOS 6.4	6.4.0 through 6.4.14	Upgrade to 6.4.15 or above
FortiOS 6.2	6.2.0 through 6.2.15	Upgrade to 6.2.16 or above
FortiOS 6.0	6.0 all versions	Migrate to a fixed release

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข **(HealthCERT)** แนะนำให้ผู้ใช้งานซอฟต์แวร์ดังกล่าว**ทำการอัปเดตเวอร์ชันซอฟต์แวร์โดยเร็วที่สุด** และให้หน่วยงานเฝ้าระวังและตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน

สำหรับผู้ใช้งานที่ไม่สามารถใช้แพตชที่สำคัญเหล่านี้ได้ทันที Fortinet ได้มีการแนะนำวิธีแก้ปัญหาโดยการปิดใช้งาน SSL VPN เป็นการป้องกันภัยคุกคามที่เกิดจาก CVE-2024-21762 แบบชั่วคราว [3]

ข่าวอ้าง

1. https://www.bleepingcomputer.com/news/security/new-fortinet-rce-flaw-in-ssl-vpn-likely-exploited-in-attacks/
2. https://securityonline.info/cve-2024-21762-cvss-9-6-fortios-ssl-vpn-zero-day-pre-auth-rce-flaw/?expand_article=1
3. https://www.fortiguard.com/psirt/FG-IR-24-015

TLP CLEAR

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (HealthCERT)

เว็บไซต์ข่าวสาร : cyber.moph.go.th

เว็บไซต์แจ้งเหตุ : health-cirt.moph.go.th

TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Fortinet เตือนถึงช่องโหว่ใน FortiSIEM

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับคุกคามทางไซเบอร์ กรณีบริษัท Fortinet ออกเตือนถึงช่องโหว่ในระดับ Critical จำนวน 2 รายการใน FortiSIEM ที่หมายเลขช่องโหว่ CVE-2024-23108 และ CVE-2024-23109 คะแนน CVSS 10 ซึ่งอาจนำไปสู่การเรียกใช้โค้ดจากระยะไกลที่สามารถรันคำสั่งที่ไม่ได้รับอนุญาตผ่านคำขอ API ที่สร้างขึ้นได้ โดยผลิตภัณฑ์ที่ได้รับผลกระทบ[1] มีดังนี้

- FortiSIEM เวอร์ชัน 7.1.0 ถึง 7.1.1
- FortiSIEM เวอร์ชัน 7.0.0 ถึง 7.0.2
- FortiSIEM เวอร์ชัน 6.7.0 ถึง 6.7.8
- FortiSIEM เวอร์ชัน 6.6 0 ถึง 6.6.3
- FortiSIEM เวอร์ชัน 6.5.0 ถึง 6.5.2
- FortiSIEM เวอร์ชัน 6.4.0 ถึง 6.4.2

โดยเดือนกุมภาพันธ์ 2567 Fortinet ได้อัปเดตคำแนะนำของปี 2566 โดยมี 2 รายการในช่องโหว่ OS Command ที่ส่งผลต่อผลิตภัณฑ์ FortiSIEM หากถูกโจมตี ช่องโหว่เหล่านี้อาจทำให้ผู้โจมตีที่ไม่ได้รับการรับรองจากระยะไกลสามารถรันคำสั่งบนระบบได้ ซึ่งเชื่อมโยงกับช่องโหว่ CVE-2023-34992 คะแนน CVSS 9.8 ที่ได้รับการแก้ไขในเดือนตุลาคม 2566

สำหรับวิธีแก้ปัญหาเบื้องต้น หน่วยงานที่ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบดังกล่าว ทาง Fortinet ได้แนะนำเกี่ยวกับวิธีการแก้ปัญหาเบื้องต้น ให้ทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่ระบุและสำหรับผู้ใช้งานที่ไม่สามารถใช้แพตช์ได้ สามารถลดช่องโหว่ได้โดยการปิดใช้งาน SSL VPN เพื่อป้องกันการโจมตี[2]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานที่ใช้งานผลิตภัณฑ์ควรเฝ้าระวังและตรวจสอบการทำงานของผลิตภัณฑ์ที่ใช้งานภายในหน่วยงาน เพื่อตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้นและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://securityaffairs.com/158813/security/fortinet-addressed-two-critical-fortisiem-vulnerabilities.html
2. https://www.fortiguard.com/psirt/FG-IR-24-015