งานพัฒนาองค์กรและขับเคลื่อนกำลังคน
รับวันที่ 18 มี.ค. 67
เวลา 14.15 น.
เลขที่รับ 368

ด่วนที่สุด บันทึกข้อความ

ส่วนราชการ กองดิจิทัลเพื่อส่งเสริมสุขภาพ กลุ่มอำนวยการ โทร. ๐ ๒๕๙๐ ๔๓๑๐

ที่ สธ ๐๙๔๙.๐๑/๗๖๑๕ **วันที่** ๑๔ มีนาคม ๒๕๖๗

เรื่อง แจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ ฉบับที่ ๖/๖๗

เรียน ประธานคณะกรรมการผู้ทรงคุณวุฒิ ผู้อำนวยการสำนักทุกสำนัก ผู้อำนวยการกองทุกกอง ผู้อำนวยการศูนย์ทุกศูนย์ ผู้อำนวยการกลุ่มทุกกลุ่ม ผู้อำนวยการสถาบันทุกสถาบัน เลขานุการกรม

ตามที่ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ได้รับมอบหมายให้มีการติดตาม เฝ้าระวังภัยคุกคามทางไซเบอร์ และเป็นศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์กรมอนามัย เพื่อเตรียมพร้อมรับมือ แก้ไขและป้องกันเหตุการณ์ภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานภายใต้สังกัดกรมอนามัย นั้น

ในการนี้ กองดิจิทัลเพื่อส่งเสริมสุขภาพ ขอแจ้งเตือนการดำเนินการเฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ รวมถึงข้อมูลข่าวสารต่าง ๆ ทั้งนี้ ให้ท่านดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานที่อาจเกี่ยวข้องกับเหตุการณ์ดังกล่าว เพื่อเป็นการยกระดับการเฝ้าระวังและป้องกันการโจมตี และลดความเสี่ยงที่อาจจะเกิดขึ้น รายละเอียดตามเอกสารแนบ หากมีข้อสงสัยสามารถสอบถามได้ที่ นายภัทร์รพี สีบุตตะ หมายเลขโทรศัพท์ ๐ ๒๕๙๐ ๔๓๑๐

จึงเรียนมาเพื่อโปรดทราบ

(นางสาวชุลีวรรณ นพวิสุทธิสกุล)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
ปฏิบัติหน้าที่ผู้อำนวยการกองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย

มอบ กสบ แจ้ง ปชส ทุกกลุ่มงาน

(นางสาวเกศรา โชคนำชัยสิริ)
(ลายเซ็นต์อิเล็กทรอนิกส์)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
รักษาราชการแทนผู้อำนวยการสถาบันพัฒนาสุขภาวะเขตเมือง

14 มีนาคม 2567

[illegible]
19 มี.ค.67
(นางสาวเกศรา โชคนำชัยสิริ)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

ทราบ
26 มี.ค.67

ThaiCERT Infoshare

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

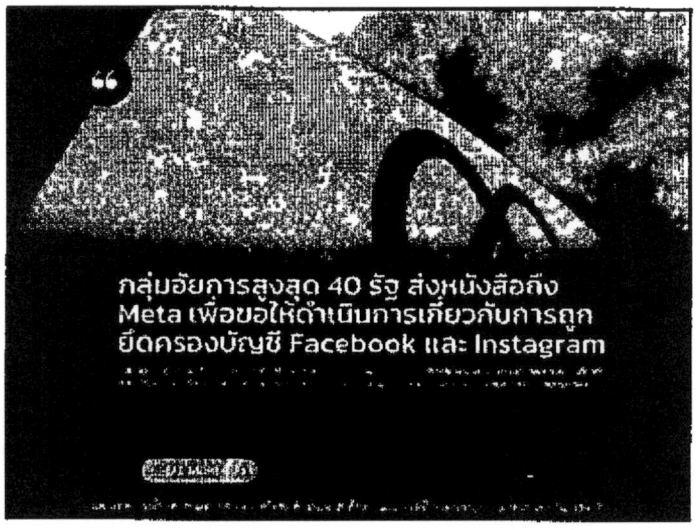
ประจำวันจันทร์ที่ 11 มีนาคม 2567

25/67(11)

NCSA สกมช

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

กลุ่มอัยการสูงสุด 40 รัฐ ส่งหนังสือถึง Meta เพื่อขอให้ดำเนินการเกี่ยวกับการถูกยึดครองบัญชี Facebook และ Instagram



กลุ่มอัยการสูงสุด 40 รัฐ ได้ส่งหนังสือถึง Meta บริษัทแม่ของ Instagram และ Facebook เพื่อแสดงถึง "ความกังวลอย่างยิ่ง" เกี่ยวกับสิ่งที่ได้รับการร้องเรียนจากผู้บริโภคที่เพิ่มขึ้นอย่างมาก เกี่ยวกับการถูกผู้ไม่ประสงค์ดีเข้ายึดบัญชีผู้ใช้และทำการเปลี่ยนรหัสผ่าน โดยเรียกร้องให้ Meta ทำหน้าที่ป้องกันให้ดีมากยิ่งขึ้น เพราะเมื่อผู้ไม่ประสงค์ดีเข้ายึดบัญชีของผู้ใช้งานแล้ว พวกเขาจะทำการเปลี่ยนรหัสผ่านทันที เพื่อให้เจ้าของเดิมเข้าใช้งานไม่ได้ และจะทำการโพสต์เนื้อหาต่าง ๆ เข้าอ่านข้อความส่วนตัว หรือติดต่อผู้ที่เกี่ยวข้องเพื่อทำการหลอกลวง และมีส่วนร่วมในสิ่งอื่นที่เป็นอันตรายหรือพฤติกรรมที่ผิดกฎหมายอื่น ๆ และนอกจากจะขอให้ Meta ดำเนินการโดยทันทีเพื่อเพิ่มกลยุทธ์การลดผลกระทบและตอบสนองต่อผู้ใช้งานที่บัญชีถูกยึดครองแล้ว ยังขอให้บริษัทให้ข้อมูลเกี่ยวกับจำนวนของการถูกยึดครองบัญชีในช่วง 5 ปีที่ผ่านมา รวมถึงข้อมูลสาเหตุที่ต้องสงสัยของการเพิ่มขึ้นของการยึดครองบัญชีและการป้องกันที่มีอยู่ด้วย

ที่มาของข่าว https://www.securityweek.com/state-ags-send-letter-to-meta-asking-it-to-take-immediate-action-on-user-account-takeovers/

ThaiCERT Infoshare

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

ประจำวันจันทร์ที่ 11 มีนาคม 25xx

วันที่ xx/xx/xxxx

NCSA สกมช

สำนักงานพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

QNAP แก้ไขช่องโหว่จำนวน 3 รายการ ใน NAS devices รวมถึงช่องโหว่ Authentication bypass

QNAP แก้ไขช่องโหว่จำนวน 3 รายการ ใน Network Attached Storage (NAS) devices ที่สามารถถูก exploit ในการเข้าถึง device ได้ โดยมีช่องโหว่ 3 รายการดังนี้

- CVE-2024-21899 เป็นช่องโหว่ improper authentication ที่อาจทำให้ผู้ใช้งานสามารถ compromise ความปลอดภัยของระบบผ่านทางเครือข่ายได้
- CVE-2024-21900 เป็นช่องโหว่ injection อาจทำให้ผู้ใช้ที่ได้รับการตรวจสอบสิทธิ์สามารถ execute command ผ่านเครือข่ายได้
- CVE-2024-21901 เป็นช่องโหว่ SQL injection อาจทำให้ผู้ดูแลระบบที่ได้รับการรับรองความถูกต้องสามารถ inject malicious code ผ่านเครือข่ายได้

QNAP แนะนำให้ผู้ใช้งานอัปเดต QTS, QuTS hero, QuTScloud และ myQNAPcloud เป็นเวอร์ชันต่อไปนี้ .

- QTS 5.1.3.2578 build 20231110 และเวอร์ชันที่ใหม่กว่า
- QTS 4.5.4.2627 build 20231225 และเวอร์ชันที่ใหม่กว่า
- QuTS hero h5.1.3.2578 build 20231110 และเวอร์ชันที่ใหม่กว่า
- QuTS hero h4.5.4.2626 build 20231225 และเวอร์ชันที่ใหม่กว่า
- QuTScloud c5.1.5.2651 และเวอร์ชันที่ใหม่กว่า
- myQNAPcloud 1.0.52 (24/11/2023) และเวอร์ชันที่ใหม่กว่า

ที่มาของข่าว https://securityaffairs.com/160217/iot/qnap-nas-products-flaws.html

ThaiCERT Infoshare

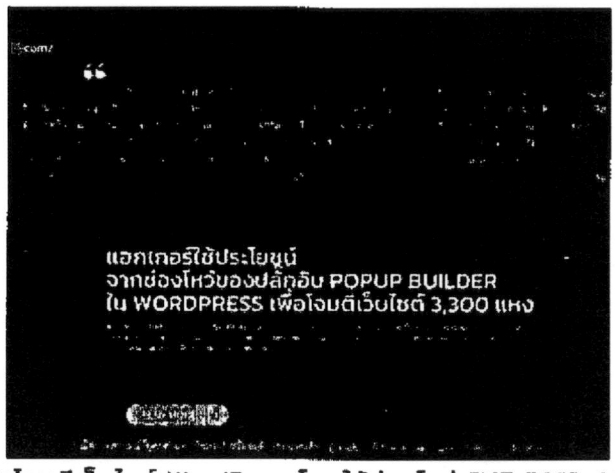
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

ประจำสัปดาห์ที่ 13 มีนาคม 2567

NCSA สกมช

สำนักงานพัฒนาธุรกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

แฮกเกอร์ใช้ประโยชน์จากช่องโหว่ของปลั๊กอิน POPUP BUILDER ใน WORDPRESS เพื่อโจมตีเว็บไซต์ 3,300 แห่ง



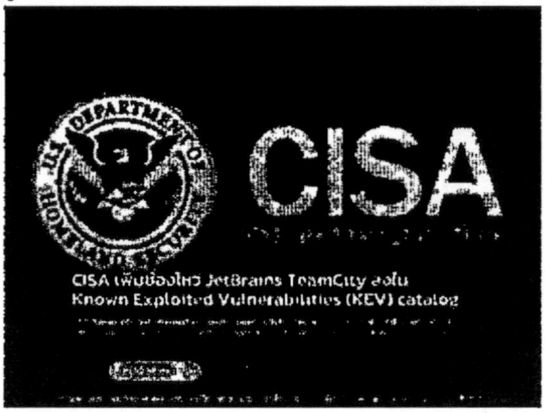
พบแฮกเกอร์กำลังโจมตีเว็บไซต์ WordPress โดยใช้ช่องโหว่ CVE-2023-6000 ที่อยู่ในปลั๊กอิน Popup Builder เวอร์ชันเก่า โดยเริ่มจากในเดือนมกราคม นักวิจัยของ Sucuri รายงานว่าพบมัลแวร์ Balada Injector โจมตีเว็บไซต์ WordPress มากกว่า 7,100 แห่ง โดยใช้ช่องโหว่ของปลั๊กอิน Popup Builder ใน WordPress เวอร์ชันที่มีช่องโหว่ ตามรายงานระบุว่าในวันที่ 13 ธันวาคม แคมเปญ Balada Injector เริ่มแพร่ระบาดไปยังเว็บไซต์โดยใช้ Popup Builder เวอร์ชันเก่า (CVE-2023-6000 , CVSS คะแนน 8.8) ปลั๊กอิน POPUP BUILDER ก่อนเวอร์ชัน 4.2.3 ซึ่งในช่วงสามสัปดาห์ที่ผ่านมา นักวิจัยสังเกตเห็นว่ามีการโจมตีเพิ่มขึ้นอย่างรวดเร็วจากแคมเปญมัลแวร์ใหม่ ซึ่งเช่นเดียวกันนี้ใช้ประโยชน์จากช่องโหว่เดียวกันใน Popup Builder จากข้อมูลของ PublicWWW ผู้เป็นภัยคุกคามได้โจมตีเว็บไซต์มากกว่า 3,300 แห่งแล้ว และเครื่องสแกนมัลแวร์ระยะไกล SiteCheck ของ Sucuri ก็ได้ตรวจพบมัลแวร์ Balada Injector บนเว็บไซต์มากกว่า 1,170 แห่ง โดยการโจมตีเหล่านี้เกิดขึ้นจาก 2 โดเมนที่จดทะเบียนเมื่อวันที่ 12 กุมภาพันธ์ 2024 คือ ttincoming.traveltraffic[.]cc และ host.cloudsonicwave[.]com โดยผู้คุกคามจะใช้ประโยชน์จากช่องโหว่ในปลั๊กอิน Popup Builder เพื่อแทรกโค้ดที่เป็นอันตรายในส่วน Custom JS หรือ CSS ของอินเทอร์เฟซผู้ดูแลระบบ WordPress ซึ่งจัดเก็บไว้ภายในในตารางฐานข้อมูล wp_postmeta ดังนั้น ผู้ดูแลเว็บไซต์ที่ใช้ปลั๊กอิน Popup Builder ควรเร่งทำการอัปเกรดให้เป็นเวอร์ชันล่าสุดทันที และหากผู้ดูแลระบบของเว็บไซต์ WordPress ที่ติดมัลแวร์อยู่แล้ว จะต้องทำการลบการแทรกที่เป็นอันตรายออกจากส่วน "Custom JS หรือ CSS" ของ Popup Builder ในอินเทอร์เฟซผู้ดูแลระบบของ WordPress จากนั้น จะต้องสแกนเว็บไซต์ในระดับไคลเอนต์และเซิร์ฟเวอร์เพื่อค้นหาแบ็คดอร์เว็บไซต์ที่ซ่อนอยู่และทำการลบออกทันที

ที่มาของข่าว https://securityaffairs.com/160329/hacking/wordpress-popup-builder-plugin-bug.html

ThaiCERT Infoshare
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
ประจำวันอังคารที่ 12 มีนาคม 2567
98/67(ท)

สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

CISA เพิ่มช่องโหว่ JetBrains TeamCity ลงใน Known Exploited Vulnerabilities (KEV) catalog



US Cybersecurity and Infrastructure Security Agency (CISA) ได้เพิ่มช่องโหว่ CVE -2024-27198 (คะแนน CVSS 9.8) เป็นการ bypass authentication ของ JetBrains TeamCity ลงใน Known Exploited Vulnerabilities (KEV) catalog โดยนักวิจัย Rapid7 ได้เปิดเผยช่องโหว่ที่สำคัญใหม่สองรายการที่ CVE-2024-27198 (คะแนน CVSS: 9.8) และ CVE-2024-27199 (คะแนน CVSS: 7.3) ใน JetBrains TeamCity On-Premises ซึ่งทำให้ผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่เพื่อควบคุมระบบที่ได้รับผลกระทบได้ดังนี้
- CVE-2024-27198 เป็นช่องโหว่ในการ bypass authentication ใน web component ของ TeamCity ที่เกิดขึ้นจาก path traversal และมีคะแนน CVSS : 9.8 (Critical)
- CVE-2024-27199 เป็นช่องโหว่ในการ bypass authentication ใน web component ของ TeamCity ที่เกิดขึ้นจาก path traversal และมีคะแนน CVSS 7.3 (High)

ช่องโหว่ดังกล่าวส่งผลกระทบต่อ TeamCity On-Premises ทั้งหมดจนถึงเวอร์ชัน 2023.11.3 โดยได้รับการแก้ไขแล้วในเวอร์ชัน 2023.11.4 โดยทั้งสองถูกค้นพบโดย Stephen Fewer นักวิจัยหลักด้านความปลอดภัยของ Rapid7 ซึ่งถูกเปิดเผยตามนโยบายการเปิดเผยช่องโหว่ของ Rapid7

ตามที่ Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities โดยหน่วยงาน FCEB จะต้องแก้ไขช่องโหว่ภายในวันที่กำหนด เพื่อป้องกันการถูกโจมตีและใช้ประโยชน์จากช่องโหว่ใน catalog ซึ่งผู้เชี่ยวชาญได้แนะนำให้องค์กรเอกชนตรวจสอบ catalog เพื่อแก้ไขช่องโหว่ในโครงสร้างพื้นฐานด้วย และทาง CISA ได้สั่งให้หน่วยงานรัฐบาลกลางแก้ไขช่องโหว่นี้ภายใน 28 มีนาคม 2024

ที่มาของข่าว https://securityaffairs.com/160236/security/jetbrains-teamcity-bug-cisa-known-exploited-vulnerabilities-catalog.html