ประชุมชี้แจงแนวทางการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

วันที่ 18 มกราคม 2566 เวลา 10.30 – 12.30 น.
ณ ห้องประชุม FOCUS อาคาร 2 ชั้น 1
สำนักงานปลัดกระทรวงสาธารณสุข
และประชุมผ่านสื่ออิเล็กทรอนิกส์ด้วยโปรแกรม
Cisco WebEx Meeting

ระเบียบวาระการประชุม

ชี้แจงแนวทางการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

ระเบียบวาระที่ 1

เรื่องที่ประธานแจ้งให้ที่ประชุมทราบ

ระเบียบวาระที่ 2

เรื่องเพื่อทราบ

2.1 สถานการณ์การแฝงเว็บไซต์พนันออนไลน์

2.2 จุดอ่อนหรือช่องโหว่สำคัญ

ระเบียบวาระที่ 3

มาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

3.1 มาตรการระดับประเทศ

3.2 มาตรการจากส่วนกลาง

3.3 มาตรการเชิงพื้นที่

ระเบียบวาระที่ 4

Show Case

เรื่องที่ประธานแจ้งให้ที่ประชุมทราบ

เรื่องเพื่อทราบ 2.1 สถานการณ์การแฝงเว็บไซต์พนันออนไลน์

สถิติการแฝงเว็บไซต์พนันออนไลน์

ลำดับ	กระทรวง	Domain name	รวม 20 ธ.ค. 65	รวม 6 ม.ค. 66	เปรียบเทียบ
1	กระทรวงสาธารณสุข	MoPH.go.th	8,834,200	4,078,800	ลดลง
2			3,577,600	3,138,100	ลดลง
3			1,282,730	1,817,990	เพิ่มขึ้น
4			60,522	1,775,560	เพิ่มขึ้น
5			2,797,000	1,230,390	ลดลง
6			665,000	1,505,170	เพิ่มขึ้น
7			2,419,900	861,800	ลดลง
8			5,313,490	578,000	ลดลง
9			504,600	445,300	ลดลง
10			378,815	369,300	ลดลง
11			198,170	251,570	เพิ่มขึ้น
12			24,200	238,900	เพิ่มขึ้น
13			40,247	22,121	ลดลง
14			8,129	17,970	เพิ่มขึ้น
15			10	121	เพิ่มขึ้น
16			110	72	ลดลง
17			34	61	เพิ่มขึ้น
18			7	2	ลดลง
19			2	2	เท่าเดิม
20			35,215	0	ลดลง
รวม			26,139,981	16,331,229	ลดลง

หมายเหตุ : ข้อมูลจาก สกมช.

เรื่องเพื่อทราบ 2.1 สถานการณ์การแฝงเว็บไซต์พนันออนไลน์

เรื่องเพื่อทราบ 2.1 สถานการณ์การแฝงเว็บไซต์พนันออนไลน์

วิเคราะห์สภาพปัญหา

1. หลายหน่วยงานขาดบุคลากรที่สามารถพัฒนาเว็บไซต์ให้มีความมั่นคงปลอดภัยและยังขาดความรู้ความเข้าใจในการพัฒนาเว็บไซต์ให้มีความมั่นคงปลอดภัยทั้งในส่วนที่พัฒนาเอง และการใช้บริการจากผู้พัฒนาเว็บไซต์และระบบที่เกี่ยวข้องที่ไม่ได้มาตรฐาน
2. หน่วยงานขาดอุปกรณ์ในการป้องกันและเฝ้าระวัง เช่น Web Application Firewall
3. หน่วยงานส่วนใหญ่ไม่มีการปรับปรุงแก้ไขปัญหาในกรณีที่เว็บไซต์มีช่องโหว่
4. ยังไม่มีมาตรฐานเรื่องการพัฒนาเว็บไซต์ที่มีความมั่นคงปลอดภัย
5. หลายหน่วยงานยังไม่ปฏิบัติตามประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
6. ยังไม่มีหน่วยงานรองรับการทำหน้าที่ Sectoral CERT หน่วยงานภาครัฐ (GovCERT)
7. ขาดการพัฒนาบุคลากรที่มีความสามารถในการทำ Secure Coding และการบริหารจัดการระบบให้ปลอดภัย

เรื่องเพื่อทราบ 2.2 จุดอ่อนหรือช่องโหว่สำคัญ

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

NCERT
Infoshare beta version
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

TLP:CLEAR

ประจำวันอังคารที่ 27 ธันวาคม 2565

ช่องโหว่ร้ายแรงของ Linux Kernel ส่งผลกระทบต่อเซิร์ฟเวอร์ SMB ที่เปิดใช้งาน ksmbd

ช่องโหว่ Linux kernel ที่สำคัญ (คะแนน CVSS เท่ากับ 10) ทำให้เซิร์ฟเวอร์ SMB ที่เปิดใช้งาน ksmbd สามารถแฮ็กได้ โดย ksmbd เป็นเซิร์ฟเวอร์ kernel ของ Linux ที่ใช้โปรโตคอล SMB3 ในพื้นที่ kernel สำหรับการแชร์ไฟล์ผ่านเครือข่าย ผู้โจมตีจากระยะไกลที่ไม่ได้รับการพิสูจน์ตัวตนสามารถรันโค้ดโดยอำเภอใจบนการติดตั้ง Linux Kernel ที่มีช่องโหว่

ช่องโหว่นี้ถูกค้นพบเมื่อวันที่ 26 กรกฎาคม 2022 โดยนักวิจัย Arnaud Gatignol, Quentin Minster, Florent Saudel, Guillaume Teissier จากทีม Thalium ที่ Thales Group และเผยต่อสาธารณะเมื่อวันที่ 22 ธันวาคม 2022

นักวิจัย Shir Tamari หัวหน้าฝ่ายวิจัยของ Wiz_IO กล่าวว่าเซิร์ฟเวอร์ SMB ที่ใช้ Samba จะไม่ได้รับผลกระทบ นอกจากนี้เขายังเสริมว่าเซิร์ฟเวอร์ SMB ที่ใช้ ksmbd มีความเสี่ยงที่จะอ่านข้อมูลได้ ซึ่งอาจทำให้หน่วยความจำของเซิร์ฟเวอร์รั่วไหล (คล้ายกับช่องโหว่ Heartbleed)

เรื่องเพื่อทราบ 2.2 จุดอ่อนหรือช่องโหว่สำคัญ

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

NCERT Infoshare
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

TLP:CLEAR

ประจำวันพฤหัสบดีที่ 12 มกราคม 2566

พบเว็บไซต์ปลอมของ AnyDesk กว่า 1,300 เว็บ เพื่อใช้แพร่กระจายมัลแวร์ Vidar

พบแคมเปญขนาดใหญ่ที่กำลังดำเนินการอยู่ ใช้โดเมนกว่า 1,300 โดเมน ที่เป็นเว็บไซต์ที่ปลอมแปลงให้ดูเหมือนเป็นเว็บไซต์ทางการของ AnyDesk โดยเว็บไซต์ทั้งหมดจะเปลี่ยนเส้นทางไปยังโฟลเดอร์ Dropbox ที่จะทำการแพร่กระจายมัลแวร์ Vidar ซึ่งมีเป้าหมายคือการขโมยข้อมูล

ซึ่ง AnyDesk เป็นโปรแกรมที่ใช้เพื่อควบคุมเครื่องคอมพิวเตอร์จากระยะไกลเพื่อดูแลระบบ ซึ่งเป็นโปรแกรมที่ได้รับความนิยมมีผู้ใช้งานนับล้านทั่วโลก และเนื่องจากความนิยมของเครื่องมือนี้จึงเกิดแคมเปญการเผยแพร่มัลแวร์ที่มักจะใช้แบรนด์ AnyDesk เพื่อให้มีผู้หลงเชื่อตกเป็นเหยื่อจำนวนมาก ยกตัวอย่างเช่น ในเดือนตุลาคม 2565 มีรายงานว่ากลุ่ม Mitsu Stealer ก็ใช้วิธีการสร้างเว็บไซต์ AnyDesk ปลอม เพื่อการฟิชชิ่งและเพื่อส่งมัลแวร์ใหม่ของตน

เรื่องเพื่อทราบ 2.2 จุดอ่อนหรือช่องโหว่สำคัญ

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

NCERT Infoshare
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

TLP:CLEAR

ประจำวันจันทร์ที่ 9 มกราคม 2566

มัลแวร์มุ่งเป้าหมายไปที่ปลั๊กอินใน WordPress ที่ไม่ได้มีการแพตช์กว่า 30 รายการ

มีการรายการปัญหาของปลั๊กอินเป็นจำนวนมาก ซึ่งหากคุณต้องการเป็นเจ้าของเว็บไซต์ตัวเอง เป็นเรื่องง่ายมากที่จะใช้ WordPress ในการสร้างเว็บไซต์ ซึ่งเป็นสัดส่วนมากกว่า 40 เปอร์เซ็นต์ของระบบในการสร้างเว็บไซต์อื่นๆ ทั้งหมดรวมกัน เหตุผลหนึ่งที่ได้รับความนิยมมากก็คือสามารถเพิ่มรูปแบบของเว็บไซต์ได้ง่ายโดยการเพิ่มปลั๊กอินที่มีอยู่หลายหมื่นรายการ แต่ทั้งนี้หากได้รับการปรับปรุงให้ทันสมัยอยู่เสมอ และได้รับการป้องกันโดยการรับรองความถูกต้องด้วยสองปัจจัย WordPress เองก็ค่อนข้างจะมีความปลอดภัยในระดับหนึ่ง ด้วยเหตุนี้ ในช่วงไม่กี่ปีที่ผ่านมา แฮกเกอร์จึงมุ่งเน้นไปที่การใช้ประโยชน์จากช่องโหว่ในปลั๊กอินมากกว่าที่จะโจมตีโดยตรง

ปลั๊กอินถูกสร้างขึ้นโดยโดยใครก็ได้ทำให้มีคุณภาพแตกต่างกันไป บางรายการมีการอัปเดตบ่อยครั้ง ในขณะที่บางรายการไม่ได้รับการสนับสนุน หรือบางรายการได้รับความนิยมมากจนถึงขั้นกลายเป็นเป็นผลิตภัณฑ์ซอฟต์แวร์ที่ประสบความสำเร็จด้วยตัวของมันเอง จนมีผู้ใช้หลายล้านคน และบางรายการอาจถูกสร้างขึ้นโดยมือสมัครเล่นคนเดียว ดังนั้น ข่าวของแคมเปญมัลแวร์ที่มุ่งเป้าหมายไปที่ปลั๊กอินที่มีช่องโหว่ที่ไม่ได้แพตช์จึงไม่น่าแปลกใจ และในความเป็นจริงแล้ว นักวิจัยกล่าวว่ามัลแวร์ที่ใช้สำหรับการโจมตีเหล่านี้อาจมีการแพร่ระบาดมาเป็นเวลาสามปีแล้ว ซึ่งตามรายงานกล่าวว่าเมื่อค้นพบเว็บไซต์ที่มีช่องโหว่ การโจมตีจะใส่สคริปต์ปลอมลงในหน้าของเว็บไซต์ โดยสคริปต์จะทำการเปลี่ยนเส้นทางผู้เยี่ยมชมเว็บไซต์ให้ไปยังเว็บไซต์ที่เป็นอันตรายเมื่อพวกเขาคลิกที่ใดก็ได้บนหน้าเว็บที่ถูกโจมตีสำเร็จแล้ว โดยรายชื่อปลั๊กอินที่มีช่องโหว่และยังไม่ได้แพตช์สามารถเข้าไปดูได้ตามลิงก์ของแหล่งข่าวที่อ้างถึง

เรื่องเพื่อทราบ 2.2 จุดอ่อนหรือช่องโหว่สำคัญ

แจ้งเตือนกรณี FORTINET ออกอัปเดตความปลอดภัย สำหรับอุปกรณ์ FORTIADC

เมื่อวันที่ 4 มกราคม 2566 Cybersecurity and Infrastructure Security Agency (CISA) ได้เผยแพร่ข้อมูลว่า Fortinet ได้ออกคำแนะนำด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ของอุปกรณ์ FortiADC[1] ในหลายเวอร์ชัน ซึ่งผู้โจมตีสามารถใช้คำสั่งที่ไม่ได้รับอนุญาตจากช่องโหว่ CVE-2022-39947[2] ซึ่งจัดเป็นช่องโหว่ระดับวิกฤตใน FortiADC เพื่อเข้าควบคุมระบบที่ได้รับผลกระทบได้ทาง Fortinet รับทราบถึงผลกระทบของช่องโหว่ดังกล่าว จึงได้ออกอัปเดตความปลอดภัย เพื่อสนับสนุนข้อมูลให้ผู้ดูแลระบบได้ดำเนินการตรวจสอบตามคำแนะนำของ Fortinet ตาม IR Number : FG-IR-22-061[3]

ทั้งนี้ ผู้ใช้งานสามารถดูรายละเอียดเพิ่มเติมที่ https://www.cisa.gov/uscert/ncas/current-activity/2023/01/04/fortinet-releases-security-updates-fortiadc

อ้างอิง

1.https://www.cisa.gov/uscert/ncas/current-activity/2023/01/04/fortinet-releases-security-updates-fortiadc
2.https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-39947
3.https://www.fortiguard.com/psirt/FG-IR-22-061

เรื่อง มาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

มาตรการระดับประเทศ

กำหนดแนวทางการแก้ไขเพื่อนำเข้าที่ประชุม กมช. เพื่อนำเสนอ ครม.

NCSA สกมช

(ร่าง) แผนการดำเนินการ

หน่วยงาน	Quick Wins (ปี 2566)	Mid Term (ปี 2567)	Long Term
สกมช. (NCSA สกมช)	• จัดทำแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ • กำกับดูแลให้หน่วยงานของรัฐ จัดทำและดำเนินการตามประมวลแนวทางปฏิบัติฯ • ดำเนินการตรวจสอบจุดอ่อนช่องโหว่ อย่างต่อเนื่อง	• กำหนดมาตรฐานการจัดทำเว็บไซต์ที่มั่นคงปลอดภัย • จัดทำหลักสูตรและการพัฒนาบุคลากรด้านไซเบอร์ ด้าน Secure Coding และการบริหารจัดการระบบให้มีความมั่นคงปลอดภัย	• ผลักดันให้ Sectoral CERT เป็นศูนย์กลางการประสานงานเฝ้าระวังป้องกัน และแชร์ข้อมูลกับ NCERT
สพร. (DGA)	• จัดตั้ง GovCERT ให้มีความพร้อมด้านบุคลากรและเครื่องมือ • จัดหา Web Application Firewall กลางเพื่อรองรับหน่วยงานภาครัฐ	• จัดทำแพลตฟอร์มเว็บไซต์ภาครัฐ ที่มีมาตรฐานความมั่นคงปลอดภัยไซเบอร์	• เฝ้าระวังความมั่นคงปลอดภัยเว็บไซต์ของหน่วยงานภาครัฐตามหน้าที่ของ GovCERT • เสริมสร้างขีดความสามารถของ GovCERT ให้เป็นไปตามประกาศ กมช. ตาม ม.50 ของ พรบ.ไซเบอร์
สพธอ. (ETDA)	• คัดเลือกบางหน่วยงานเพื่อใช้ Web App Firewall ของ สพธอ. • ทำงานร่วมกับ สกมช. เพื่อปรับปรุงมาตรฐานเว็บไซต์ภาครัฐ	• กำกับดูแลผู้ให้บริการด้านธุรกรรมทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย	• กำกับดูแลผู้ให้บริการด้านธุรกรรมทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย
หน่วยงานที่เกี่ยวข้อง	• ตรวจสอบ ติดตาม มีการปรับปรุงเว็บไซต์และรายงานตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ • ขึ้นทะเบียนเว็บไซต์เพื่อรับการตรวจสอบและเฝ้าระวังจาก สกมช. และ สพร.	• สมัครเข้าร่วมโครงการ • พัฒนาเว็บไซต์ภาครัฐ ที่มีมาตรฐานความมั่นคงปลอดภัย • ขอรับการสนับสนุนงบประมาณเพื่อจัดจ้างบุคลากรที่มีความรู้ด้านไซเบอร์	• เข้าร่วมโครงการกับ DGA

เรื่อง มาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

มาตรการจากส่วนกลาง

- จัดทำทะเบียนเว็บไซต์
- สนับสนุนการปิดโดเมนที่เป็นอันตราย
- ช่วยเฝ้าระวังภัยคุกคามทางไซเบอร์
- ให้ใช้ Domain Name ของกระทรวงสาธารณสุข ภายใต้การจัดสรรของ ศทส.สป.
- ช่องทางติดต่อ Health Cert

  โทรศัพท์ 08 1558 1924, อีเมล health-cirt@moph.go.th, Line Official: @health-cirt, Line Group: mophCIRT และเว็บไซต์แจ้งเหตุการณ์ไซเบอร์ http://health-cirt.moph.go.th
- รวมทีม CIRT ของทุกหน่วยงาน มาช่วยกันรักษาความมั่นคงปลอดภัย

เรื่อง มาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

มาตรการเชิงพื้นที่

1. สำรวจ เว็บไซต์ของหน่วยงานทั้งหมด
2. ปิด เว็บไซต์ที่ไม่ได้ใช้งาน
3. ดูแล Environments ทั้งหมดที่เกี่ยวข้อง ของเว็บไซต์
4. หาอุปกรณ์ ป้องกัน
5. เฝ้าระวัง

Show Case

THANK YOU