นกส.015/2566

10 กุมภาพันธ์ 2566

ฝ่ายนวัตกรรมการศึกษา
จุฬาลงกรณ์มหาวิทยาลัย
วันที่: 9 กุมภาพันธ์ 2566 เวลา 13:31
เลขรับที่: นกส.0186/2566

คณะแพทยศาสตร์
จุฬาลงกรณ์มหาวิทยาลัย
เลขรับที่ 02065/2566
วันที่ 9 ก.พ. 2566 เวลา 09:15

บันทึกข้อความ

ส่วนงาน สำนักบริหารเทคโนโลยีสารสนเทศ โทร. 0 2218 3314 โทรสาร 0 2218 3338

ที่ อว 64.2.11/0087 **วันที่** 9 กุมภาพันธ์ 2566

เรื่อง แจ้งเตือนกรณีมีรายงานพบแคมเปญการโจมตีด้วย RANSOMWARE จำนวนมาก

ภาควิชาอายุรศาสตร์ พศ
จุฬาลงกรณ์มหาวิทยาลัย
เลขรับที่: อย.00883/2566
ลงวันที่: 10 ก.พ. 2566 เวลา 10:32

เรียน คณบดี/ผู้อำนวยการสถาบัน/ศูนย์/สำนัก/วิทยาลัย และหน่วยงานอื่นๆ

ด้วยสำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย ได้รับการแจ้งเตือนจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.สกมช.) เกี่ยวกับกรณีของทางทีม SingCert (Singapore Computer Emergency Response Team) มีการเผยแพร่รายงานเกี่ยวกับแคมเปญแรนซัมแวร์ ที่กำลังดำเนินอยู่ โดยการใช้ประโยชน์จากช่องโหว่เก่าหมายเลข (CVE-2021-21974) ในเซิร์ฟเวอร์ VMware ESXi ที่ไม่ได้รับการแพตช์ โดยผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่เพื่อทำการโจมตีโดยการเรียกใช้โค้ดจากระยะไกล ทั้งนี้จึงขอแจ้งให้ผู้ที่ดูแลระบบดำเนินการตรวจสอบเวอร์ชันผลิตภัณฑ์ที่ได้รับผลกระทบ และอัปเดตให้เป็นเวอร์ชันล่าสุดทันที เพื่อเป็นการป้องกันจากการถูกโจมตี ดังรายละเอียดตามเอกสารแนบ

และหากทางหน่วยงานประสงค์จะทราบข้อมูลเพิ่มเติม หรือ ความช่วยเหลือใดๆ กรุณาติดต่อหน่วยประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ สำนักบริหารเทคโนโลยีสารสนเทศ โทร 83413 หรืออีเมล csirt@chula.ac.th

จึงเรียนมาเพื่อโปรดพิจารณา

(นายรุ่งโรจน์ กิตติถาวรกุล)
ผู้อำนวยการสำนักบริหารเทคโนโลยีสารสนเทศ

เรียน รองคณบดีฝ่ายนวัตกรรมการศึกษาและสารสนเทศ
เพื่อโปรดพิจารณา

(นางสุชิรา ปัญญาสันติกุล)
ผู้อำนวยการฝ่ายบริหาร
๙ กุมภาพันธ์ ๒๕๖๖

ประชาสัมพันธ์ในภาควิชา
เพื่อทราบ

(รศ.ดร.นพ.วิโรจน์ ศรีอุฬารพงศ์)
หัวหน้าภาควิชาอายุรศาสตร์
12 กุมภาพันธ์ 2566

เรียน หัวหน้าภาควิชา/หน่วยงาน
เพื่อโปรดทราบ

(รศ.นพ.วันล่า กุลวิชิต)
รองคณบดีฝ่ายนวัตกรรมการศึกษาและสารสนเทศ
9 กุมภาพันธ์ 2566

TLP:CLEAR

เอกสารการแจ้งเตือนกรณี มีรายงานพบแคมเปญการโจมตีด้วย Ransomware จำนวนมาก โดยใช้ช่องโหว่เก่าบนเซิร์ฟเวอร์ VMware ESXi ที่ไม่ได้รับการแพตช์

เอกสารการแจ้งเตือนกรณี มีรายงานพบแคมเปญการโจมตีด้วย Ransomware จำนวนมาก โดยใช้ช่องโหว่เก่าบนเซิร์ฟเวอร์ VMware ESXi ที่ไม่ได้รับการแพตช์

Singapore Computer Emergency Response Team (SingCert) มีการเผยแพร่รายงานเกี่ยวกับแคมเปญแรนซัมแวร์[1] ที่กำลังดำเนินอยู่ โดยการใช้ประโยชน์จากช่องโหว่เก่าหมายเลข (CVE-2021-21974) [2] ในเซิร์ฟเวอร์ VMware ESXi[3] ที่ไม่ได้รับการแพตช์ โดยผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่เพื่อทำการโจมตีโดยการเรียกใช้โค้ดจากระยะไกล ซึ่งเรียกว่า heap-overflow ในบริการ OpenSLP ผลิตภัณฑ์เวอร์ชัน[4] โดยมีเวอร์ชันที่ได้รับผลกระทบดังต่อไปนี้

- ESXi เวอร์ชัน 7.x ก่อนหน้า ESXi70U1c-17325551
- ESXi เวอร์ชัน 6.7.x ก่อนหน้า ESXi670-202102401-SG
- ESXi เวอร์ชัน 6.5.x ก่อนหน้า ESXi650-202102101-SG

ผู้ใช้งานและผู้ดูแลระบบของเวอร์ชันที่ได้รับผลกระทบ จึงควรอัปเดตให้เป็นเวอร์ชันล่าสุด เพื่อเป็นการป้องกันจากการถูกโจมตี[5] และขอให้ทำการตรวจสอบระบบทั้งหมด เพื่อสแกนหาสัญญาณของการบุกรุก ผู้ใช้งานและผู้ดูแลระบบควรประเมินด้วยว่าพอร์ต 427 บนระบบ ESXi สามารถปิดใช้งานได้ โดยไม่รบกวนการทำงานหรือไม่ อาจต้องกำหนดค่ากฎ Firewall โดยอ้างว่าถูกโจมตี เพื่อหยุดการเชื่อมต่อกับ ที่อยู่ IP ดังต่อไปนี้

- IP : 104.152.52[.]55
- IP : 193.163.125[.]138
- IP : 43.130.10[.]173
- IP : 104.152.52[.]0/24

ทั้งนี้ SingCert แนะนำให้ผู้ใช้งานและผู้ดูแลระบบของเวอร์ชันผลิตภัณฑ์ที่ได้รับผลกระทบควรอัปเดตเป็นเวอร์ชันล่าสุดทันที สามารถดูรายละเอียดเพิ่มเติมที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://www.csa.gov.sg/en/singcert/Alerts/AL-2023-015
2. https://www.vmware.com/security/advisories/VMSA-2021-0002.html
3. https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/
4. https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/
5. https://www.csa.gov.sg/singcert/Advisories/ad-2021-009/

TLP:CLEAR