แจ้งเตือน : ช่องโหว่

ระดับ : Critical

ระดับ : High

ผลกระทบทางธุรกิจ

- [x] Financial damage
- [x] Reputation damage
- [x] Non-compliance
- [x] Privacy violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

บริษัท ออราเคิล คอร์ปอเรชั่น ออก Security Patch ประจำเดือนมกราคม 2565 แก้ไขช่องโหว่ระดับ Critical และ High ควรติดตามและอัปเดต

วันที่แจ้งเตือน 20 มกราคม 2565

บริษัท ออราเคิล คอร์ปอเรชั่นผู้พัฒนาและผู้ให้บริการซอฟต์แวร์ระดับองค์กร (Enterprise software) และโปรแกรมและเครื่องมือบริหารจัดการฐานข้อมูล (Database Management Software/Tools) รายใหญ่ ได้ออกคำแนะนำเกี่ยวข้องกับ Security Patch ประจำเดือนมกราคม 2565 ประกอบด้วยชุดการปรับปรุงจำนวน 497 รายการที่ส่งผลกระทบต่อผลิตภัณฑ์จำนวน 165 รายการ ที่มี Security Patch สำหรับแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรงและสูง เช่น

ลำดับ	รายละเอียดช่องโหว่	หมายเลข CVE
1	ช่องโหว่ประเภท Buffer Overflow ในผลิตภัณฑ์ Oracle ที่เรียกใช้ Algorithm เข้า/ถอดรหัส แบบ SM2 จาก Openssl API ก่อให้เกิดความเสี่ยงต่อ Denial of Service หรือการใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution)	CVE-2021-3711
2	ช่องโหว่ประเภท Buffer Overflow ในผลิตภัณฑ์ Oracle ที่มีการใช้งานตัวแปรข้อมูล Python ctype (PyCArg_repr) และมีการตรวจสอบข้อมูล Input ไม่เพียงพอ ก่อให้เกิดความเสี่ยงต่อการทำ Denial of Service หรือการใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution)	CVE-2021-3177
3	ช่องโหว่ประเภท Denial of Service ต่อผลิตภัณฑ์ Oracle ที่มีการใช้องค์ประกอบของ Nginx จากการเขียนทับข้อมูลหน่วยความจำจากข้อผิดพลาด Nginx UDP DNS Resolver	CVE-2021-23017
4	ช่องโหว่ที่ Oracle e-Business Suite ที่ทำให้ผู้ที่ไม่หวังดีสามารถเข้าถึง Oracle Configurator ผ่าน Http Protocol สามารถยกระดับสิทธิเพื่อเข้าถึง แก้ไข เปลี่ยนแปลง หรือลบทำลายข้อมูลที่เข้าถึงหรือบริหารจัดการโดย Oracle Configurator ได้	CVE-2022-21255

รายชื่อซอฟต์แวร์ที่ได้รับผลกระทบ เช่นระบบบริหารจัดการทรัพยากรระดับองค์กร (ERP) ระบบและเครื่องมือบริหารจัดการฐานข้อมูล เครื่องมือวิเคราะห์ข้อมูลทางธุรกิจ และระบบบริหารจัดการเครื่องแม่ข่ายเสมือน (VM) เป็นต้น ทั้งนี้ สามารถตรวจสอบรายชื่อซอฟต์แวร์ที่ได้รับผลกระทบได้ที่ https://www.oracle.com/security-alerts/cpujan2022.html#AppendixGG

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบและพิจารณาดำเนินการอัปเดต Security Patch เพื่อแก้ไขช่องโหว่ของระบบปฏิบัติการและโปรแกรมที่ได้รับผลกระทบ
2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Security Patch ก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

แจ้งเตือน : ช่องโหว่

ระดับ : Critical

ระดับ : High

ผลกระทบทางธุรกิจ

- [x] Financial damage
- [x] Reputation damage
- [x] Non-compliance
- [x] Privacy violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

บริษัท ออราเคิล คอร์ปอเรชั่น ออก Security Patch ประจำเดือนมกราคม 2565 แก้ไขช่องโหว่ระดับ Critical และ High ควรติดตามและอัปเดต

วันที่แจ้งเตือน 20 มกราคม 2565

ข้อมูลอ้างอิง

1. https://blogs.oracle.com/security/post/january-2022-cpu
2. https://www.cisa.gov/uscert/ncas/current-activity/2022/01/18/oracle-releases-january-2022-critical-patch-update#:~:text=Oracle%20has%20released%20its%20Critical,control%20of%20an%20affected%20system.
3. https://www.tenable.com/blog/oracle-january-2022-critical-patch-update-addresses-266-cves
4. https://securityaffairs.co/wordpress/126836/security/oracle-critical-patch-update-january-2022.html