

- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability



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

วันที่แจ้งเตือน 20 เมษายน 2565

บริษัท ออราเคิล คอร์ปอเรชั่น ผู้พัฒนาและผู้ให้บริการซอฟต์แวร์ระดับองค์กร (Enterprise software) และโปรแกรมและเครื่องมือบริหารจัดการฐานข้อมูล (Database Management Software/Tools) รายใหญ่ ได้ออกคำแนะนำเกี่ยวกับ Security Patch ประจำเดือนเมษายน 2565 จำนวน 520 รายการ ที่ส่งผลกระทบต่อผลิตภัณฑ์จำนวน 175 รายการ โดยมี Security Patch สำหรับแก้ไขช่องโหว่ที่มีความรุนแรงระดับร้ายแรงและสูง เช่น

ลำดับ	รายละเอียดช่องโหว่	หมายเลข CVE
1	ช่องโหว่ประเภท Path Traversal ในผลิตภัณฑ์ Oracle ที่ทำให้ผู้ไม่หวังดีสามารถดำเนินการ Map Directory ไปยัง Directory ภายนอกที่อยู่นอกเหนือการควบคุมโดยใช้วิธีการ Alias-Like Directives ได้	CVE-2021-42013
2	ช่องโหว่ในผลิตภัณฑ์ Oracle ที่มีการใช้งานไลบรารีของ Java Application ในการเก็บข้อมูล Log ของซอฟต์แวร์ Apache (Apache Log4j)	CVE-2022-23305
3	ช่องโหว่ประเภท Denial of Service ต่อผลิตภัณฑ์ Oracle ที่มีการใช้องค์ประกอบของ Nginx จากการถูกโจมตีโดยการเขียนทับข้อมูลหน่วยความจำที่เกิดจากข้อผิดพลาด Nginx UDP DNS Resolver	CVE-2021-23017
4	ช่องโหว่ในผลิตภัณฑ์ Oracle ที่มีการใช้งาน Module Core ของ Java Spring Framework สำหรับพัฒนา Java Web Application	CVE-2022-22965

รายชื่อซอฟต์แวร์ที่ได้รับผลกระทบ เช่น ระบบบริหารจัดการทรัพยากรระดับองค์กร (ERP) ระบบและเครื่องมือบริหารจัดการฐานข้อมูล เครื่องมือวิเคราะห์ข้อมูลทางธุรกิจ และระบบบริหารจัดการเครื่องแม่ข่ายเสมือน (VM) เป็นต้น ทั้งนี้ สามารถตรวจสอบรายชื่อซอฟต์แวร์ที่ได้รับผลกระทบได้ที่ <https://www.oracle.com/security-alerts/cpuapr2022.html#AppendixDB>

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

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

แจ้งเตือน : ช่องโหว่

ระดับ : Critical

ระดับ : High

ผลกระทบทางธุรกิจ

- Financial damage
- Reputation damage
- Non-compliance
- Privacy violation

ผลกระทบต่อระบบ

- Loss of Confidentiality
- Loss of Integrity
- Loss of Availability

TLP Color : White



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

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

วันที่แจ้งเตือน 20 เมษายน 2565

#### ข้อมูลอ้างอิง

- <https://www.cisa.gov/uscert/ncas/current-activity/2022/04/19/oracle-releases-april-2022-critical-patch-update>
- <https://www.oracle.com/security-alerts/>
- <https://www.helpnetsecurity.com/2022/04/08/april-2022-patch-tuesday-forecast/>
- <https://securityaffairs.co/wordpress/126836/security/oracle-critical-patch-update-january-2022.html>