

- Financial Damage
- Reputation Damage
- Non-Compliance
- Privacy Violation

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



แจ้งเตือนช่องโหว่ระดับร้ายแรง (Critical) บนโปรแกรม VMware Cloud Director (CVE-2022-22966)

วันที่แจ้งเตือน 21 เมษายน 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนเกี่ยวกับช่องโหว่ระดับร้ายแรง (Critical) บนโปรแกรม VMware Cloud Director ซึ่งเป็นโปรแกรมสำหรับบริหารและจัดการ Virtual Data Centre Management Data Centre Expansion และ Cloud Migration (CVE-2022-22966) มีช่องโหว่ให้ผู้ไม่หวังดีที่มีบัญชีผู้ใช้งาน (Authenticated User) และได้รับสิทธิที่เกี่ยวข้อง (High Privileged Malicious Actor) ที่เข้าถึงระบบทั้งในส่วนของผู้เช่า (Tenant) หรือส่วนของผู้ให้บริการ (Provider) สามารถส่งและเรียกใช้คำสั่งอันตรายจากระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution) และเข้าควบคุมระบบ Cloud Computing ได้

ทั้งนี้ เวอร์ชันที่ได้รับผลกระทบได้แก่ -10.1.X 10.2.X และ 10.3.X

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1. ตรวจสอบและพิจารณาดำเนินการอัปเดต Security Patch เวอร์ชัน 10.1.4.1 10.2.2.3 และ 10.3.3 เพื่อแก้ไขช่องโหว่โปรแกรม VMware Cloud Director ซึ่งสามารถรายละเอียดเพิ่มเติมได้ที่

- <https://www.vmware.com/security/advisories/VMSA-2022-0013.html>

External Link

2. ผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบการติดตั้ง Security Patch ก่อนนำไปใช้งานจริง

ข้อมูลอ้างอิง

External Link

- 1) <https://nvd.nist.gov/vuln/detail/CVE-2022-22966>
- 2) <https://digital.nhs.uk/cyber-alerts/2022/cc-4078>
- 3) <https://thehackernews.com/2022/04/critical-vmware-cloud-director-bug.html#comment-box>
- 4) <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22966>