

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

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



ช่องโหว่ในผลิตภัณฑ์ Cisco, MS SharePoint, MongoDB Server และ Check Point หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 23 กันยายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า ช่องโหว่ในผลิตภัณฑ์ Cisco, Microsoft SharePoint, MongoDB Server และ Check Point หลายรายการ เสี่ยงถูกนำไปใช้ในการโจมตีระบบสารสนเทศขององค์กร ได้แก่

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Cisco	- ช่องโหว่ CVE-2026-76460 เป็นช่องโหว่ประเภท Authentication Bypass ใน Cisco Identity Services Engine (ISE) เกิดจากการควบคุมขั้นตอนการยืนยันตัวตนที่ไม่ถูกต้อง ส่งผลให้ผู้ไม่หวังดีสามารถโจมตีได้จากระยะไกลโดยข้ามกระบวนการยืนยันตัวตน จากนั้นสามารถส่ง Request ที่สร้างขึ้นไปยัง API ด้วยสิทธิ์ระดับ Root และทำการซ่อนหรือลบ Indicators of Compromise (IoCs) ในระบบได้ - Cisco แนะนำให้ผู้ผลิตผลิตภัณฑ์ ดำเนินการติดตั้งและอัปเดตซอฟต์แวร์เป็นเวอร์ชันที่แก้ไขช่องโหว่แล้วตามทีระบุในอ้างอิง 2	ส่งผลกระทบต่อผลิตภัณฑ์ Cisco ISE และ Cisco ISE Passive Identity Connector (ISE-PIC) เวอร์ชัน 3.1, 3.2, 3.3, 3.4 และ 3.5

ข้อมูลอ้างอิง Cisco

- <https://nvd.nist.gov/vuln/detail/cve-2026-76460>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5>
- <https://www.securityweek.com/active-exploitation-triggers-emergency-patch-for-cisco-ise-zero-day/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ในผลิตภัณฑ์ Cisco, MS SharePoint, MongoDB Server และ Check Point หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 23 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Microsoft	• ช่องโหว่ CVE-2026-65660 เป็นช่องโหว่ประเภท Code Injection ใน Microsoft SharePoint เกิดจากการตรวจสอบ SafeControls ไม่เพียงพอ โดยกระบวนการของ ToolPane ที่ประมวลผล Web Part Markup ไม่ได้ Escape เครื่องหมาย (") ในค่าของ Attribute ที่ถูกต้อง ทำให้ผู้ไม่หวังดีสามารถแทรกคำสั่งที่สร้างขึ้น และนำไปใช้ร่วมกับช่องโหว่ประเภท Authentication Bypass เพื่อทำการโจมตีเพิ่มเติมได้ • Microsoft แนะนำให้ผู้ใช้ผลิตภัณฑ์ดังกล่าว อัปเดตเป็นซอฟต์แวร์เวอร์ชันแก้ไขที่ระบุไว้แล้ว	ส่งผลกระทบต่อผลิตภัณฑ์ • MS SharePoint Server Subscription Edition เวอร์ชัน 16.0.5565.1001 และต่ำกว่า • MS SharePoint Server 2019 เวอร์ชัน 16.0.10417.20198 และต่ำกว่า • MS SharePoint Enterprise Server 2016 เวอร์ชัน 16.0.19725.20522 และต่ำกว่า

ข้อมูลอ้างอิง Microsoft

1. <https://nvd.nist.gov/vuln/detail/cve-2026-65660>
2. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>
3. <https://thehackernews.com/2026/09/sharepoint-flaw-initially-listed-as.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

ผลกระทบต่อระบบ

☒ Loss of Confidentiality

☒ Loss of Integrity

☒ Loss of Availability

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ช่องโหว่ในผลิตภัณฑ์ Cisco, MS SharePoint, MongoDB Server และ Check Point หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 23 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
MongoDB Server	ช่องโหว่ CVE-2026-82067 - ช่องโหว่นี้เกิดจากการทำงานผิดพลาดของส่วนตรวจสอบการตั้งค่า (Configuration Validation Component) ภายใน MongoDB Server ส่งผลให้ระบบยืนยันตัวตน (Authorization Subsystem) อาจถูกปิดการใช้งานได้โดยไม่ได้ตั้งใจระหว่างกระบวนการ Server Startup - ส่งผลให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ์เป็นผู้ดูแลระบบ ควบคุมการทำงานของเครื่องเป้าหมาย ติดตั้งซอฟต์แวร์หรือมัลแวร์ รวมถึงการเข้าถึงหรือแก้ไขข้อมูลภายในระบบ แนวทางป้องกันและแก้ไข - แนะนำให้ผู้ใช้งาน อัปเดต MongoDB Server เวอร์ชันล่าสุดที่ได้รับการแก้ไขแล้วโดยเร็ว - ตรวจสอบการตั้งค่าความปลอดภัยของฐานข้อมูล เช่น ตรวจสอบว่าเปิดใช้งานการยืนยันตัวตน (Authentication) อยู่หรือไม่ ตรวจสอบสิทธิ์ของบัญชีผู้ใช้งาน จำกัดการเข้าถึง MongoDB เฉพาะระบบหรือ เครือข่ายที่จำเป็น เป็นต้น - หากพบว่า MongoDB Server มีความเสี่ยง ให้ดำเนินการตรวจสอบเหตุการณ์ทันที เช่น การสร้างบัญชีผู้ดูแลระบบโดยไม่ได้รับอนุญาต การเปลี่ยนแปลงสิทธิ์ผู้ใช้งาน และการส่งออกข้อมูล (Data Exfiltration) เป็นต้น	ส่งผลกระทบต่อ MongoDB Server - เวอร์ชัน 7.0 ต่ำกว่า 7.0.41 - เวอร์ชัน 8.0 ต่ำกว่า 8.0.30 - เวอร์ชัน 8.3 ต่ำกว่า 8.3.9

ข้อมูลอ้างอิง MongoDB

1. <https://nvd.nist.gov/vuln/detail/cve-2026-82067>
2. <https://www.mongodb.com/docs/manual/release-notes/>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

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



ช่องโหว่ในผลิตภัณฑ์ Cisco, MS SharePoint, MongoDB Server และ Check Point หลายรายการเสี่ยงถูกใช้ในการโจมตี

วันที่แจ้งเตือน 23 กันยายน 2569

ผู้ผลิต	รายละเอียดช่องโหว่	ผลิตภัณฑ์ที่ได้รับผลกระทบ
Check Point	• ช่องโหว่ CVE-2026-93616 เป็นช่องโหว่ประเภท Path Traversal Vulnerability ในส่วนของหน้าเว็บบริหารจัดการ (management server's web service) ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงไฟล์ หรือ โฟลเดอร์ได้ และอาจทำการอัปโหลดและรันสคริปต์บนระบบได้โดยไม่ต้องพิสูจน์ตัวตน • Check Point ออกแพตช์แก้ไขเมื่อวันที่ 22 กันยายน 2026 ผู้ดูแลระบบควรตรวจสอบเวอร์ชันและ Jumbo Hotfix Take ที่ใช้งาน และทำการติดตั้งแพตช์ล่าสุด รวมถึงตรวจสอบ Indicators of Compromise (IoCs) และร่องรอยการโจมตีตามคำแนะนำของ Check Point	เวอร์ชันที่ได้รับผลกระทบ ได้แก่ • R82.20 (no Jumbo Hotfix installed) • R82.10 with Jumbo Hotfix Take 44 or below • R82 with Jumbo Hotfix Take 126 or below • R81.20 with Jumbo Hotfix Take 166 or below • R81.10 with Jumbo Hotfix Take 190 or below (end of support) • R81, R80.40, R80.30, R80.20, R80.10 and R80 (all end of support)

ข้อมูลอ้างอิง Check Point

- <https://nvd.nist.gov/vuln/detail/cve-2026-93616>
- <https://thehackemews.com/2026/09/check-point-warns-of-management-server.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ

