

NCTICC INTELLIGENCE BULLETIN

New Microsoft Defender 'ShieldCrash' zero-day grants SYSTEM access

New Microsoft Defender 'ShieldCrash' zero-day grants SYSTEM access

Document ID:	PB-2569-1276
Classification:	TLP:WHITE — Public Distribution
Issued:	09 September 2026 / 11:55 ICT
Author:	NCTICC Threat Intelligence Section
Distribution:	Public — Government Agencies / Critical Infrastructure
Reference:	https://ctithai.work/portal/docs/PB-2569-1276

1. EXECUTIVE SUMMARY

NCTICC analyst summary of public BleepingComputer report. New Microsoft Defender 'ShieldCrash' zero-day grants SYSTEM access Original source URL: <https://www.bleepingcomputer.com/news/security/new-microsoft-defender-shieldcrash-zero-day-grants-system-access/> This bulletin captures the public-facing summary of the referenced threat. Detailed indicators (IOCs, TTPs, MITRE ATT&CK; mappings) are available to authenticated NCTICC federation members in the corresponding TLP:AMBER analyst product. Operators should follow vendor guidance from the original source while NCTICC enrichment is in progress.

สรุปบทวิเคราะห์รายงานจากแหล่งสาธารณะของ NCTICC จาก BleepingComputer หัวข้อ: New Microsoft Defender 'ShieldCrash' zero-day grants SYSTEM access ลิงก์ต้นฉบับ: <https://www.bleepingcomputer.com/news/security/new-microsoft-defender-shieldcrash-zero-day-grants-system-access/> รายงานย่อนี้รวบรวมข้อมูลภาพรวมจากรายงานสาธารณะ ตัวบ่งชี้ภัยคุกคามโดยละเอียด (IOC, TTP, การ map ATT&CK;) จะปรากฏใน ผลิตภัณฑ์ระดับ TLP:AMBER สำหรับสมาชิกที่มีการยืนยันตัวตน หน่วยงานสามารถดำเนินการตามคำแนะนำของผู้ผลิตในรายงานต้นฉบับ ระหว่างที่ NCTICC ดำเนินการ enrichment ต่อไป

2. KEY OBSERVATIONS

- แหล่งข่าวต้นฉบับ: BleepingComputer
- URL: <https://www.bleepingcomputer.com/news/security/new-microsoft-defender-shieldcrash-zero-day-grants-system-access/>
- วันที่ในแหล่งต้นฉบับ: 2026-09-09
- สถานะ enrichment: รอการประมวลผลโดยทีมวิเคราะห์

3. RECOMMENDED ACTIONS

- ตรวจสอบรายละเอียดเพิ่มเติมจากลิงก์ต้นฉบับ
- ฝังระวัง IOC ที่เกี่ยวข้องผ่านระบบ SIEM/EDR ของหน่วยงาน
- รายงานกิจกรรมที่สงสัยว่าเกี่ยวข้องไปยัง NCTICC ทาง security@ctithai.work

ANNEX A — INDICATORS OF COMPROMISE (IOC)

Full IOC list (~400 entries) is available via the authenticated NCTICC Portal. Click here to [view encrypted IOC annex](#) (requires NCTICC personnel authentication). Mirror: <https://764e2766d2b3447c.cdn.ctithai.work/iocs>

A latest version of this document with revision-764e27 is available. [Check for updates](#).

4. CONTACT / ติดต่อ

NCTICC Operations Center (24/7)

Email: ncticc-ops@ctithai.work

CERT: ncticc-cert@ctithai.work

Portal: <https://ctithai.work/portal>

Document verification: <https://ctithai.work/verify/764e2766d2b3447c>

Document reference: 764e2766d2b3447c — please retain for citation.