8 Januari 2026

Advaes namba 111: Vulnerabiliti long saed blong *Race Condition* blong *Microsoft Windows*

Deit we hemi rilis:	12 Novemba 2025
Impak:	HAE / KRITIKOL
TLP:	KLIA

Dipatmen blong Komunikesen mo Dijitol Transfomesen (DKDT) tru long CERT Vanuatu (CERTVU), i givimaot advaeseri ia.

Woning ia hem i blong olgeta Oganaesesen mo Sistem/Netwok Administreta we oli yusum prodak ia. Woning ia oli mekem blong olgeta teknikol yusa mo sistem administreta oli andastanem.

Wanem ia?

CVE-2025-62215 – hem i wan *race-condition* (*improper synchronization*) wiknes o vulnerabiliti we i stap insaed long *windows kernel*. Blong mekem i klia, plante denja o proses oli aksesem wan kernel risos we oli serem witaot stret *synchronization*, we i mekem se wan lokol ataka i eskeletem ol privilej.

Hemia i afektem wanem Sistem?

Hem i afektem:

- Hem i afektem sapot edisen blong Windows 10, Windows 11, mo Windows Server (inkludum ol niufala vesen).
- Ol sistem we oli stap ranem ol kernel vesen kasem (be i no finis ia nomo) sam vesen we oli pajem, oli wik o vulnerebol.

- From hemia hem i wan vulnerabiliti long level blong kernel, eni wokstesen o seva wea wan yusa i save eksekutum kod long hem (o oli tekem haf kontrol long hem finis), hem i stap long risk blong privilej eskelesen.

Hemia i minim wanem?

Olsem wanem ol ataka oli eksploitem vulnerabiliti ia (atak vekta):

- Ataka i mas gat sam level blong lokol kod eksekusen o akses blong save eksploitem vulnerabiliti ia (olsem eksampol wan yusa akaon o proses). Vulnerabiliti ia hem i no rimot fulwan from zero akses.
- Ataka i kosem *race-condition* tru long fasin blong eksekutum operesen we i stap happen semtaem agensem kernel risos we oli serem blong koraptem memori o mekem *synchronization* i no go gud. Hemia i save lid i go long ol eskelesen privilej.
- Taem hem i go antap, ataka bae save tekem ful kontrol blong sistem, go raon long ol aplikesen kontrol, disebolem ol sekiuriti aspek, instolem ol bakdoa, muv i go kros, o yusum kompromaes host olsem steping ston.

Proses blong Katem Daon Risk

CERTVU i rikomendem se:

Mekem pajing kwiktaem – Aplaem *Microsoft November 2025 Patch Tuesday*

Sipos pajing i no save tekem ples kwiktaem:

- Limitim ol yusa akaon: mekem sua blong gat smol namba blong lokol yusa privilej nomo
- Monitarem ol sistem blong faenem ol eskelesen indikesen we i no nomol blong lokol privilej
- Limitim o disebolem ol sistem we oli alaowem ol yusa blong lodem o eksekutum ol kod we oli no trastem – Hemia i katem daon atak.

Refrens

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-62215