Celah Keamanan “ShieldBreak” Ancam Pengguna Windows Defender

Category: TEKNOLOGI
written by Redaksi | August 13, 2026

SEANTERONEWS.com – Keamanan sistem operasi Windows kembali diuji setelah seorang peneliti keamanan independen yang dikenal dengan alias “Nightmare Eclipse” mengungkap kerentanan zero-day pada Windows Defender. Celah yang diberi nama “ShieldBreak” ini memungkinkan penyerang untuk melakukan eskalasi hak akses ke tingkat “SYSTEM” tingkat otoritas tertinggi dalam sistem operasi Windows.

Penemuan ini menjadi alarm bagi jutaan pengguna Windows 11 25H2 dan Windows Server 2025. Meskipun ShieldBreak tidak dapat digunakan untuk meretas komputer dari jarak jauh secara langsung, celah ini sangat berbahaya bagi penyerang yang sudah memiliki akses awal ke dalam sistem untuk mengambil alih kontrol penuh perangkat.

Sebagai bentuk pembuktian, Nightmare Eclipse telah merilis kode proof-of-concept (PoC) yang memungkinkan publik menguji kerentanan tersebut. Dua pakar keamanan siber terkemuka, Will Dormann dan Kevin Beaumont, telah mengonfirmasi bahwa kode tersebut bekerja efektif pada versi Windows 11 terbaru.

“Ini memberikan hak akses SYSTEM dari akun pengguna biasa mana pun. Saya telah mencobanya, dan ini benar-benar berfungsi di Windows 11 versi terbaru,” ungkap Beaumont melalui media sosialnya.

ShieldBreak sendiri diduga muncul setelah peneliti yang sama berhasil membobol tambalan (patch) sebelumnya untuk kerentanan serupa bernama “Rogue Planet” yang sempat diperbaiki Microsoft pada Juni lalu. Peneliti tersebut mengeklaim telah menemukan metode alternatif untuk melewati proteksi yang sudah diberikan Microsoft.

Sosok Nightmare Eclipse diketahui merupakan mantan karyawan Microsoft yang merasa kecewa atas perlakuan perusahaan di masa lalu. Hal ini memicu konflik personal yang membuat sang peneliti enggan melakukan koordinasi atau pengungkapan kerentanan secara bertanggung jawab (coordinated vulnerability disclosure), sebuah standar industri yang biasanya dilakukan untuk memberi waktu perusahaan menambal celah sebelum dipublikasikan.

Tindakan publikasi PoC secara terbuka ini sempat memicu kontroversi. Sebelumnya, Microsoft sempat memberi isyarat akan menempuh jalur hukum bagi siapa pun yang mempublikasikan kode eksploitasi tanpa koordinasi, namun perusahaan kemudian melunak setelah mendapat kritik keras dari komunitas keamanan siber.

Menanggapi laporan mengenai ShieldBreak, Microsoft menyatakan bahwa mereka saat ini tengah melakukan investigasi menyeluruh. “Microsoft menyadari adanya kerentanan yang dilaporkan dan sedang menyelidiki validitas serta potensi dampaknya terhadap

pelanggan. Kami berkomitmen untuk melakukan penyelidikan isu keamanan dan memperbarui produk terdampak secepat mungkin," jelas juru bicara Microsoft kepada PCMag.

Hingga saat ini, belum tersedia pembaruan resmi dari Microsoft untuk memperbaiki celah ShieldBreak. Para ahli keamanan menyarankan pengguna untuk tetap waspada, menghindari akses ke situs atau file yang mencurigakan, dan terus memantau pembaruan keamanan resmi yang nantinya akan dirilis melalui Windows Update.[]