



Tanggal 15 Juli 2026



PANDUAN KEAMANAN CVE-2026-50412

DESKRIPSI UMUM

CVE-2026-50412 merupakan kerentanan keamanan dengan tingkat keparahan tinggi pada Microsoft Windows NTFS yang disebabkan oleh *Stack-based Buffer Overflow*. Kerentanan ini memungkinkan penyerang lokal dengan hak akses rendah mengeksploitasi kelemahan pada proses pengolahan sistem berkas NTFS sehingga dapat menjalankan kode arbitrer dengan hak akses SYSTEM. Eksploitasi kerentanan ini dapat mengakibatkan *Elevation of Privilege*, yang memungkinkan penyerang memperoleh kendali penuh terhadap sistem target.

[CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C]

VERSI SISTEM TERDAMPAK

- Windows 10 (1607, 1809, 21H2, 22H2)
- Windows 11 (24H2, 25H2, 26H1)
- Windows Server (2012/2012R2/2016/2019/2022/2025)

7.8
(High)



REKOMENDASI

- Pembaruan Patch:** Segera pasang pembaruan keamanan Windows Juli 2026 yang mencakup perbaikan CVE-2026-50412 sesuai versi sistem operasi yang digunakan. Pastikan perangkat telah menggunakan build yang telah diperbaiki oleh Microsoft.
- Hak Terbatas (Least Privilege):** Batasi hak akses pengguna dengan menggunakan akun non-administrator untuk aktivitas sehari-hari. Langkah ini dapat mengurangi risiko Elevation of Privilege apabila kerentanan berhasil dieksploitasi.
- Mitigasi Sistem:** Aktifkan fitur keamanan bawaan Windows, seperti Data Execution Prevention (DEP), Control Flow Guard (CFG), atau Windows Exploit Protection, untuk membantu mencegah eksekusi kode berbahaya.
- Pemantauan dan Deteksi:** Lakukan pemantauan terhadap log keamanan Windows serta aktivitas yang berkaitan dengan NTFS. Gunakan solusi EDR atau antivirus yang mampu mendeteksi indikasi eksploitasi maupun perilaku mencurigakan.

SUMBER REFERENSI

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-50412>
- <https://app.opencve.io/cve/CVE-2026-50412>

