MEMORY OUT-OF-BOUND READ / WRITE

DESCRIPTION

Missing size and boundary checking cause more data then excepted flooded into the memory, resulting in illegal execution or memory data leakage

ATTACK VECTOR

Lengthy and special crafted input. Attack Codes: a_M0 a_M1 a_M2 a_M3 a_S3 a_W3

CONSEQUENCE

Illegal execution or leaking of data in memory. Defence Codes: d_D0 d_D1 d_D6 d_D7 d_D9 d_D10 d_D11 d_E0 d_E1 d_M4 d_M7 d_M14 d_P2 d_P3 d_P5

v_C13