NVD DB Update

CVE-2021-45423 - Score: 9.8

Components:

pev project pev 0.81

Description:

A Buffer Overflow vulnerabilityexists in Pev 0.81 via the pe_exports function from exports.c.. The array offsets_to_Names is dynamically allocated on the stack using exp->NumberOfFunctions as its size. However, the loop uses exp->NumberOfNames to iterate over it and set its components value. Therefore, the loop code assumes that exp->NumberOfFunctions is greater than ordinal at each iteration. This can lead to arbitrary code execution.

Main problems:

120 "Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')"

https://cybersword.tech
www.linkedin.com/in/cybersword-tech
ph1sher
@davidwowa