Every crash is a potential security vulnerability

devblogs.microsoft.com/oldnewthing/20081230-00

December 30, 2008

Raymond Chen

Whenever I post about a programming error that can lead to crashes, the security team gets all excited and starts looking for ways to exploit it. For example, when I wrote about the fundamentally flawed `DONT_RESOLVE_DLL_REFERENCES` flag, the security folks went scouring through the Windows source code looking for anybody who passed that flag, and then tried to come up with ways they could trick the code into loading an unintended DLL and causing trouble.

I wouldn't have known about this exercise at all if one of the team members hadn't forwarded me some email discussing their preliminary investigations as if to say, "See what you started?"

Raymond Chen

Follow