STATUS_BUFFER_OVERFLOW really should be named STATUS_BUFFER_OVERFLOW_PREVENTED

devblogs.microsoft.com/oldnewthing/20080404-00

April 4, 2008

Raymond Chen

One category of dubious security vulnerability that comes into the security response team is people who recently discovered the `STATUS_BUFFER_OVERFLOW` status code.

> **Title**: Buffer overflow occurs in scenario X
>
> **Description**: Run a file monitoring tool and perform scenario X. In the log, you will see entries that have the error `STATUS_BUFFER_OVERFLOW`. This is an easily reproducible buffer overflow bug.

If only the system were so smart that it could detect buffer overflows in this way. But what you're seeing is not actual a buffer overflow. The status code `STATUS_BUFFER_OVERFLOW` does not mean that a buffer overflow has occurred; rather, it means that the buffer passed by the application was too small to hold all the requested data. Its name should really be `STATUS_BUFFER_OVERFLOW_PREVENTED` or `STATUS_INSUFFICIENT_BUFFER`. Indeed, the corresponding Win32 error code has the less misleading name `ERROR_INSUFFICIENT_BUFFER`.

Every wannabe security investigator sees this error code in a monitoring tool and says "Jackpot!" And then they send a report to the security response team and brag about it to their friends. "Dude, I found two dozen buffer overflows in just a few minutes. I am so 31337!"

Raymond Chen

Follow