What's a CVE ?

22nd Feb 2022, Limerick, Ireland.

What's a CVE ?

No, nothing to do with a resume extradonaire …just another acronym I'm afraid and this time it stands for **C**ommon **V**ulnerability & **E**xposures. *What ?* Simply put, a CVE is a publicly known cybersecurity vulnerability in a particular piece of software. A cybersecurity vulnerability is a "weak-link" and depending on where it may be found, it can impact you or your organisations IT security and possibly leave you open to exploitation by cybercriminals. For example: https://www.bleepingcomputer.com/news/security/attackers-now-actively-targeting-critical-sonicwall-rce-bug/.

CVE.ORG and partners discover, identify, categorise, assign and publish a database of vulnerabilities each with a unique identity number and severity level. CVE.ORG is American run and funded by the US Department of Homeland Security (yeah, that's right…you remember Carrie & Saul in the TV show Homeland? That's where they worked too … more counter-terrorism though than code-reviewing 😊).

Why should I care ?

CVEs exist for all most all software including Windows, macOS, Android, iOS and a whole host of others including Linux, Apache, MySQL, PHP, Python and the GCC Compiler Toolchains.

CVEs may ("probably") exist in the software that you provide to your customers. In some cases, that may be due to the code written by your developers, in others, vulnerabilities maybe introduced by the software development toolchains or third-party software that your developers use. Whilst a CVE can exist in a compiler it can also exist in a run-time library which of course is particularly problematic as that library may end up being linked in as part of your application which goes to your customers.

Most security conscious organisations take CVEs very seriously and have systems and procedures in place to identify known CVEs in the software that they use, and, in some cases, they will not adopt or use software containing certain CVEs. There are several third-party companies providing software to "detect" and "categorise" CVEs such as Synopsys Black Duck which one of our leading customers use to ensure that all GCC Compiler Toolchain deliveries from Ashling are "clean" from any CVEs above a certain severity level. Cleaning (or remediation) in this context requires Ashling identifying and removing CVEs before every Toolchain release to the customer thus meeting their security requirements and keeping the world a slightly safer place.

Thanks for reading.

Hugh @ Ashling.