**Vulnerability management of open source and third-party SW components in automotive industry – Open source és 3rd party SW kódok sérülékenységének kezelése autóiparban**

A modern gépjárművek kialakítása egyre komplexebb számítástechnikai rendszereken alapulnak, melyek szinte folyamatosan kapcsolatban állnak privát és publikus hálózaton elérhető szolgáltatásokkal.

Ez a hálózatba kapcsolt kialakítás növeli a rendszer kiberbiztonsági sebezhetőségét, amelyeket kihasználva rosszindulatú támadók akár emberéleteket is veszélyeztethetnek.

A gépjárművekben megjelenő kiberbiztonsági kockázatokat kezelni kell, melyre törvényi előírások (UN-ECE155 és UN-ECE156) és szabályozói folyamatok kerültek kialakításra (ISO21434, ISO24089) az autóiparban.

Ennek a kockázatkezelési folyamatnak egy kiemelt eleme a kódban található ismert sérülékenységek kezelése, a gépjármű teljes életciklusa során, a törvényi előírásoknak és vevői követelményeknek megfelelően.

A SW fejlesztés során felhasznált open source és 3rd party SW-eket pontosan fel kell térképezni, strukturáltan tárolni, hogy az azokhoz tartozó ismert és jövőben feltárt sérülékenyégek azonosításra kerüljenek.

A megismert sérülékenyéghez tartozó kockázatokat kezelni kell, illetve a feltárt sérülékenységre adott kockázatkezelést a vevők fele jogi és üzleti igények alapján ismertetni kell.

A témakiírás célja ennek a folyamatnak a kidolgozása és a szükséges rendszerek kialakítása.