

CRIME PREVENTION & INFORMATION CENTER (CPIC)
CYBER SECURITY ALERT



(U) Note: The following information is based on reporting from public media outlets that are external to the Chicago Police Department's Crime Prevention & Information Center (CPIC). The CPIC takes reasonable care in linking websites but has no direct control over the content of the linked sites or the changes that may occur to the content on those sites. The information provided by this brief is for situational awareness and should be handled in accordance with the recipient's intelligence oversight and information handling procedures.

CYBER VULNERABILITES –AUTOMOTIVE INDUSTRY

(U//FOUO) Publication of cyber vulnerabilities to automotive industry published on open source site.

(U//FOUO) On January 3, 2023 a self-described security consultant, hacker, and bug bounty hunter published an article titled “Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More”, on open source platforms. The publication is a compilation of car hacking research discussing vulnerabilities affecting multiple vehicle brands and automotive industry companies.

(U//FOUO) The publication claims the ability to remotely compromise vehicle software and operations via SIM cards installed on multiple brands of vehicles, access personal identifiable information and geo location history of vehicles through automotive industry web sites.

(U//FOUO) Implications to law enforcement.

(U//FOUO)) Alleged vulnerabilities to GPS vehicle tracking and sensor systems connected to vehicles have the potential to impact to law enforcement and emergency services since these devices are often installed on police cars and ambulances.

(U) This is a Cyber Alert and has not finally evaluated intelligence. It is being shared for informational purposes but has not been fully evaluated, integrated with other information, interpreted or analyzed. This information is being provided for your situational awareness and safety.