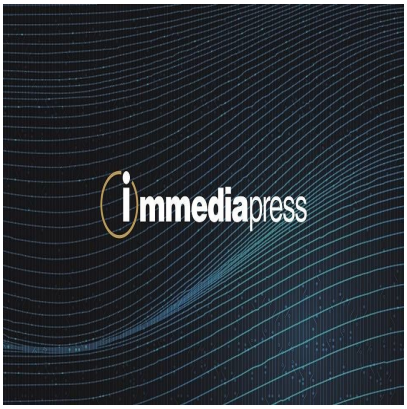

Kaspersky individua falle di sicurezza nei sistemi delle auto moderne

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Milano 29 ottobre 2025

Durante il Security Analyst Summit 2025, Kaspersky ha presentato i risultati di un audit di sicurezza che ha portato alla scoperta di una grave vulnerabilitÃ in grado di consentire lâ??accesso non autorizzato a tutti i veicoli connessi di un produttore automobilistico.

Sfruttando una vulnerabilitÃ zero-day in unâ??applicazione di un appaltatore accessibile al pubblico, i cybercriminali sono riusciti a ottenere il controllo del sistema telematico dei veicoli, compromettendo la sicurezza fisica di automobilisti e passeggeri. In alcuni casi, gli aggressori avrebbero potuto forzare il cambio di marcia o spegnere il motore mentre il veicolo era in movimento. Questi risultati mettono in luce gravi carenze nella sicurezza informatica del settore automotive e sollecitano lâ??adozione di misure di protezione piÃ¹ efficaci.

Produttore automobilistico

Lâ??audit di sicurezza Ã¨ stato condotto da remoto e ha riguardato i servizi accessibili al pubblico del produttore automobilistico e lâ??infrastruttura dellâ??appaltatore, per cui Kaspersky ha individuato diversi servizi web esposti. Inizialmente, sfruttando una vulnerabilitÃ zero-day di tipo SQL injection presente in unâ??applicazione Wiki (una piattaforma web che permette agli utenti di creare, modificare e gestire contenuti in modalitÃ collaborativa), gli esperti sono riusciti a estrarre lâ??elenco degli utenti del fornitore con gli hash delle loro password, alcune delle quali sono state decifrate a causa di una policy di sicurezza debole. Questa violazione ha consentito lâ??accesso al sistema di tracciamento dei progetti dellâ??appaltatore (uno strumento software utilizzato per gestire e monitorare attivitÃ , bug o

problemi allâ??interno dei progetti), che conteneva dettagli di configurazione sensibili sullâ??infrastruttura telematica del produttore automobilistico, incluso un file contenente gli hash delle password degli utenti di uno dei server telematici dei veicoli. Nei veicoli moderni, la telematica consente la raccolta, la trasmissione, lâ??analisi e lâ??utilizzo di diversi tipi di dati, come velocitÃ , posizione geografica e molto altro.

Il veicolo connesso

Per quanto riguarda il veicolo connesso, Kaspersky ha scoperto un firewall configurato in modo errato che esponeva i server interni del veicolo. Utilizzando una password di un account di servizio acquisita in precedenza, i ricercatori sono riusciti ad accedere al file system del server tramite le credenziali fornite da un altro appaltatore, ottenendo cosÃ¬ il controllo completo dellâ??infrastruttura telematica. In particolare, Ã¨ stato individuato un comando di aggiornamento del firmware che ha permesso agli esperti di caricare un firmware modificato nella Telematics Control Unit (TCU). Questo ha consentito lâ??accesso al bus CAN (Controller Area Network) del veicolo, un sistema che collega diverse componenti, come motore e sensori. Successivamente, Ã¨ stato possibile accedere a vari altri sistemi, tra cui motore e trasmissione, permettendo la potenziale manipolazione di numerose funzioni critiche dellâ??auto, con conseguente rischio per la sicurezza di conducente e passeggeri.

â??Le vulnerabilitÃ della sicurezza derivano da problemi molto comuni nel settore automobilistico: servizi web accessibili al pubblico, password deboli, assenza di autenticazione a due fattori (2FA) e archiviazione di dati sensibili non crittografati. Questa violazione dimostra come un singolo punto debole nellâ??infrastruttura di un fornitore possa compromettere lâ??intero sistema dei veicoli connessi. Lâ??industria automobilistica deve dare prioritÃ a pratiche di sicurezza informatica solide, in particolare per i sistemi di terze parti, al fine di proteggere i conducenti e mantenere la fiducia nelle tecnologie dei veicoli connessiâ?•,ha commentato Artem Zinenko, Head of ICS CERT Vulnerability Research and Assessment di Kaspersky.

Kaspersky raccomanda ai fornitori di limitare lâ??accesso a Internet dei servizi web tramite VPN, assicurandosi che tali servizi siano separati dalla rete aziendale. Suggerisce inoltre di applicare rigorose policy per le password, implementare lâ??autenticazione a due fattori, proteggere i dati sensibili e integrare la registrazione con un sistema SIEM per il monitoraggio in tempo reale.

Per i produttori automobilistici, Kaspersky consiglia di limitare lâ??accesso alla piattaforma telematica dal segmento di rete del veicolo, utilizzando liste di autorizzazione per le interazioni di rete, disabilitando lâ??autenticazione tramite password SSH, eseguendo i servizi con privilegi minimi e garantendo lâ??autenticitÃ dei comandi nelle TCU, oltre a integrare il monitoraggio tramite SIEM.

Kaspersky ICS CERT

Kaspersky ICS CERT si occupa principalmente di identificare e affrontare sia le potenziali minacce che quelle esistenti nei sistemi di automazione industriale e nellâ??Industrial Internet of Things (IIoT). Il team ha identificato e contribuito a eliminare con successo centinaia di vulnerabilitÃ presenti in prodotti

e componenti ICS diffusi, migliorando la sicurezza e la resilienza di questi sistemi critici contro sofisticati attacchi informatici.

Seguici su:

Tweets by KasperskyLabIT

http://www.facebook.com/kasperskylabitalia

https://www.linkedin.com/company/kaspersky-lab-italia

https://www.instagram.com/kasperskylabitalia/

https://t.me/KasperskyItalia

Informazioni su Kaspersky

Kaspersky Ã¨ unâ??azienda globale di cybersecurity e privacy digitale fondata nel 1997. Con oltre un miliardo di dispositivi protetti dalle minacce informatiche emergenti e dagli attacchi mirati, la profonda esperienza di Kaspersky in materia di sicurezza e di Threat Intelligence si trasforma costantemente in soluzioni e servizi innovativi per la sicurezza di aziende, infrastrutture critiche, governi e consumatori in tutto il mondo. Il portfolio completo dellâ??azienda comprende una protezione Endpoint leader, prodotti e servizi di sicurezza specializzati e soluzioni Cyber Immune per contrastare le minacce digitali sofisticate e in continua evoluzione. Aiutiamo oltre 200.000 aziende a proteggere ciÃ² che piÃ¹ conta per loro. Per ulteriori informazioni Ã¨ possibile consultare https://www.kaspersky.it/

Contatti:
Immediapress
Contatto di redazione:
NoesisKaspersky Italia

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Immediapress

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Ottobre 29, 2025
Autore
redazione