DATA STORED IN VEHICLE INFOTAINMENT SYSTEMS

OVERVIEW

Data stored in vehicle infotainment systems in government, corporate, and rental vehicles could contain sensitive information such as call logs, contacts, addresses, travel routes, and other personally identifiable information (PII). When vehicles are serviced by or sold to third parties, there is a possibility the data from the vehicle's infotainment system could be extracted and used by criminals for nefarious purposes.

VEHICLE INFOTAINMENT SYSTEMS

Many vehicles used today by government and corporate employees have the capability to sync information from our mobile devices to the vehicle's infotainment systems. This usually occurs when an employee connects their cellular or mobile devices to the vehicle via Bluetooth, Wi-Fi, or USB. Most of the time this is done for convenience reasons so employees can more easily complete tasks while driving, such as making phone calls or using GPS applications for travel. However, government agencies and businesses should be aware that syncing mobile devices to the vehicle infotainment system could also sync PII and other sensitive information related to an employee's work and personal life.

Figure 1: Vehicle infotainment system display

SECURITY CONCERNS

If data from a vehicle's infotainment system is not property deleted, the following information could be accessed by another party:

- Call logs, text messages, and contacts
- Routes and times traveled, searched locations, home and work addresses, and other historical and saved location data
- Media files, including voice memos, voicemails, photos, and videos
- Bluetooth/handset ID, phone information, driver information, and garage door access codes

This information could be used by malicious actors to re-construct an employee's travel or to learn more about the employee's company, contacts, and private life.

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED. ***Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.***

RECOMMENDATIONS

It is recommended that prior to the vehicle being returned or sold, the proper methods are taken to ensure that all user data is deleted from the vehicle's infotainment system. Most car companies have published guides on how to reset a vehicle's infotainment system to factory settings. Please refer to the "Related Information" heading below for instructions published by Ford, General Motors, and Chrysler.

Drivers should be aware of information left on the vehicle's infotainment system when a vehicle is taken to a repair facility for maintenance, as this information can be quickly accessed without any trace. The Michigan Cyber Command Center recommends all vehicle maintenance should only be conducted by trusted partners of your organization.

Lastly, it is important to keep in mind that despite factory resetting the vehicle's infotainment system, there may still be some advanced methods that can be used by malicious actors to forensically extract deleted user data. If this is a concern, it is further recommended to consult with a trained forensic expert to ensure all sensitive and PII is removed from the vehicle prior to selling or turning it in.

RELATED INFORMATION

- https://owner.ford.com/support/how-tos/sync/sync-with-navigation/setup/how-to-perform-a-master-reset.html
- https://www.chevrolet.com/how-to/infotainment
- https://www.gmc.com/entertainment-and-connectivity
- https://www.driveuconnect.com/support/chrysler.html

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED. ***Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.***