



# **Volkswagen & Audi Data Breach Jun - 2021**

---

- BY AISHWARYA JADHAV
- FALL 2021

# Impact

---

- Volkswagen Group of America, Inc. (VWGoA) disclosed a data breach in Jun 2021
- Vendor left Audi, Volkswagen, and some authorized dealer's data unsecured on the Internet
- More than 3.3 million customers and interested buyer's impacted (5 million records exposed)
- Users across USA and Canada are affected
- Customer Names, email ids, addresses, phone numbers, Vehicle Identification Numbers (VIN), information about the driver, and vehicle information is exposed
- Stolen data ranged from year 2014 to 2019

# Overview


---

- Data made available to be purchased on a hacking forum
- \$4,000 and \$5,000 for the whole database
- Hacker published 2 samples of the data, which contained names, email ids, mailing addresses, and phone numbers.
- Hacker [000] along with another hacker Badhou3a developed a script to scan the internet for exposed Azure blobs container and fetch data
- Blob container were left unsecured by the vendor sometime between August 2019 and May 2021
- Anyone who knew the required URLs could access the stored information without authentication
- Microsoft Azure Blob - stores massive amounts of unstructured data
- Cloud storage private by default but Files can be stored without any access restrictions as well


# Published Data


SELLING

audiusa.com 2019 5m

by  - June 14, 2021 at 10:42 PM

New Reply









Posts830



Threads65

JoinedNov 2017


Reputation2,143

3 YEARS OF SERVICE



 June 14, 2021 at 10:42 PM This post was last modified: 1 hour ago by  dited 4 times in total. #1

I'm back from my break and got some leaks init fam

Shoutout @ badhou3a for helping

<https://www.zdnet.com/article/volkswagen...ed-buyers/>  
<https://www.vice.com/en/article/xgxaq4/h...volkswagen>

Audiausa.com Analytics Dump  
Has VINS Emails Names and more  
2 Files & Backup

Leads.csv  
Lines: 3,862,231  
Sample: <https://skidbin.net/>  
Sample with numbers: <https://skidbin.net/>  
Data: Created,FirstName,LastName,Address1,Address2,City,State,ZipCode,HomePhone,E  
mailAddress & more

Sale.csv  
Lines: 1,792,278

# How?

---

- Fetch data using URL: `http://<storage>.blob.core.windows.net/<container>/<file>`
- Variables in the Blob storage URL – storage account, container name and file/blob name
- Guess the storage names and sent a DNS Resolver query to a DNS server
- If IP matches with our URL, we know the storage account exists
- Based on the storage accounts, make a logical list of possible container names
- Send HTTP request “List Blobs” which returns a list of the blobs under the specified container to the storage account endpoint.

**Note: Only containers with the ‘Public read access for container and its blobs ’ access level will allow this kind of request for an unauthorized client.**

**Anyone having access to the link can access the data without any authorization check!**

# Action & Advice

---

- Emails or letters are sent to the victims by the company, providing free credit monitoring and warning them that they may receive phishing attacks using the stolen data.
- Data was left unsecure for very long time therefore all communications claiming to be from Audi or Volkswagen should be treated suspiciously, especially email or SMS text messages.
- For sensitive exposed data, freeze credit report to make it harder for third parties to perform identity theft and take credit under victims name.

# Similar Events

---

## Raven Fishing [Jul - 2021]

- 0.2 million customers data containing names, addresses, genders, phone numbers, email ids, customer IDs, delivery dates, shipping fees, payments, and shipment tracking numbers

## Presumably Microsoft Dynamics [Jan - 2021] (Based on the content of the leaked files)

- 3,800+ files containing Business pitches; product descriptions, product code, hardcoded password

## Cayman Islands bank [Dec - 2020]

- Backups covering a \$500 million investment portfolio including personal banking information, passport data and even online banking PINs

## CRM customers of a UK firm [Dec - 2020]

- 0.5 million documents containing occupational health assessments, insurance claim, backed-up emails, letters, spreadsheets, screenshots, and more.

## Tesco [Sept - 2019]

- Parking web app exposed tens of Millions of Automatic Number Plate Recognition (ANPR) Image

# References

---

<https://cybersecuritynews.com/hackers-audi-volkswagen/>

<https://www.analyticsinsight.net/top-10-worst-data-breaches-in-2021/>

<https://heimdalsecurity.com/blog/the-stolen-data-of-audi-and-volkswagen-is-being-sold-on-a-hacking-forum/>

<https://www.bleepingcomputer.com/news/security/audi-volkswagen-data-breach-affects-33-million-customers/>

<https://heimdalsecurity.com/blog/audi-and-volkswagen-involved-in-a-massive-data-breach/>

<https://www.bleepingcomputer.com/news/security/audi-volkswagen-customer-data-being-sold-on-a-hacking-forum/>

[https://www.theregister.com/2021/07/27/azure\\_blob\\_raven\\_hengelsport/](https://www.theregister.com/2021/07/27/azure_blob_raven_hengelsport/)

[https://www.theregister.com/2020/12/18/probase\\_unsecured\\_azure\\_blob/](https://www.theregister.com/2020/12/18/probase_unsecured_azure_blob/)

<https://threatpost.com/cayman-islands-bank-records-exposed-azure-blob/161729/>

<https://thedataprivacygroup.com/blog/2019-9-23-tesco-shutters-parking-app-following-license-plate-image-leak/>

<https://www.vpnmentor.com/blog/report-microsoft-dynamics-leak/>

<https://www.cyberark.com/resources/threat-research-blog/hunting-azure-blobs-exposes-millions-of-sensitive-files>





# Thank you!

---

ANY QUESTIONS?