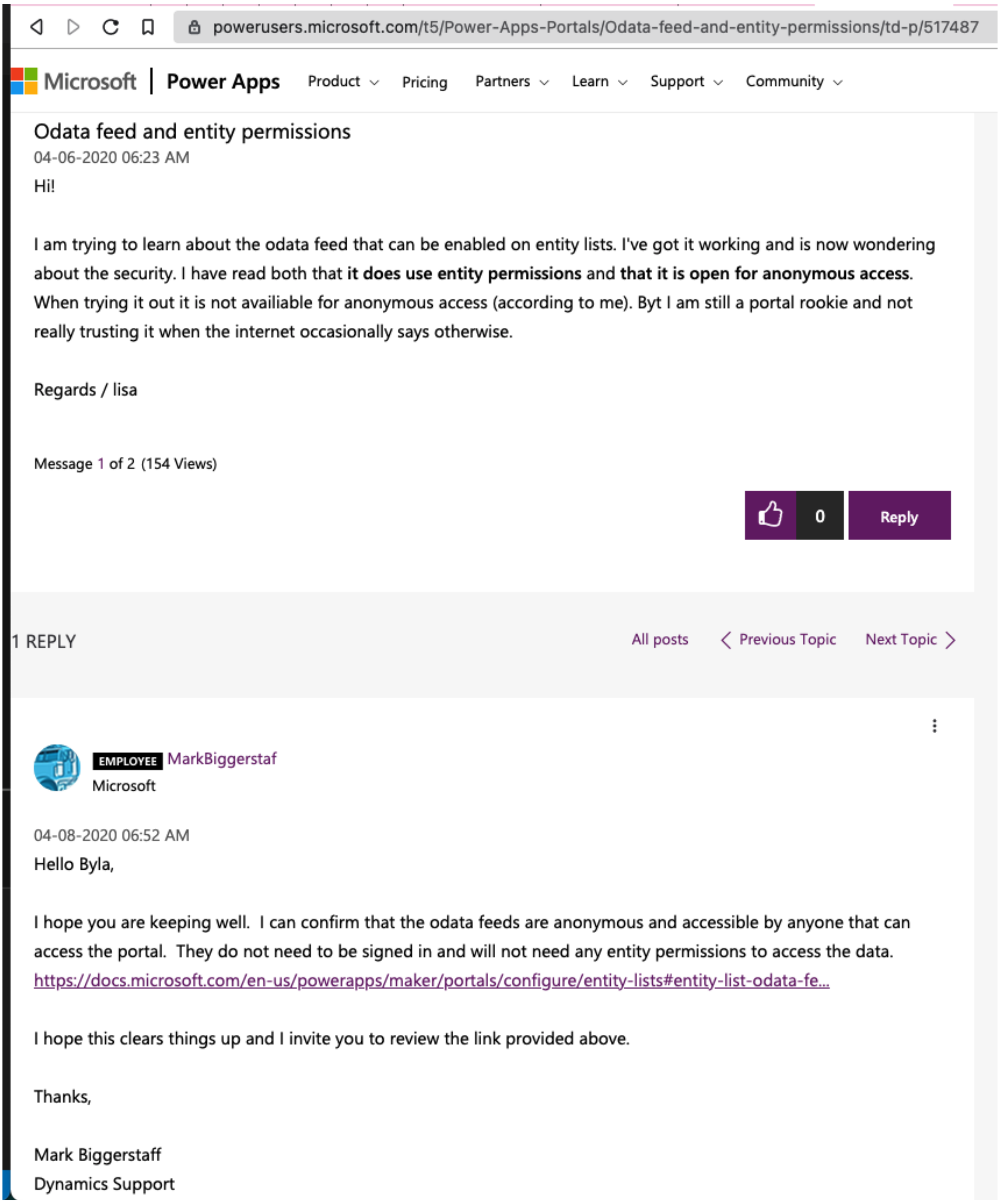
UpGuard

By Design: How Default Permissions on Microsoft Power Apps Exposed Millions

The UpGuard Research team can now disclose multiple data leaks resulting from Microsoft Power Apps portals configured to allow public access - a new vector of data exposure. The types of data varied between portals, including personal information used for COVID-19 contact tracing, COVID-19 vaccination appointments, social security numbers for job applicants, employee IDs, and millions of names and email addresses. UpGuard notified 47 entities of exposures involving personal information, including governmental bodies like Indiana, Maryland, and New York City, and private companies like American Airlines, J.B. Hunt, and Microsoft, for a total of 38 million records across all portals. This research presents an example of a larger theme, which is how to manage third-party risks (and exposures) posed by platforms that don't slot neatly into vulnerability disclosure programs as we know them today, but still present as security issues.

Product documentation for Power Apps describes the conditions under which OData APIs can be made publicly accessible, and the main Power Apps marketing page lists the ability to access “your data either anonymously or through commercial authentication” as one of the top features. In cases like registration pages for COVID-19 vaccinations, there are data types that should be public, like the locations of vaccination sites and available appointment times, and sensitive data that should be private, like the personally identifying information of the people being vaccinated.

The number of accounts exposing sensitive information, however, indicates that the risk of this feature– the likelihood and impact of its misconfiguration– has not been adequately appreciated. On one hand, the product documentation accurately describes what happens if an app is configured in this way. On the other hand, empirical evidence suggests a warning in the technical documentation is not sufficient to avoid the serious consequences of misconfiguring OData list feeds for Power Apps portals. Our conversations with the entities we notified suggested the same conclusion: multiple governmental bodies reported performing security reviews of their apps without identifying this issue, presumably because it has never been adequately publicized as a data security concern before. In publishing this report we aim to make other security practitioners aware of the risk associated with configuring OData APIs for Power Apps portals so that such exposures can be prevented in the future.


powerusers.microsoft.com/t5/Power-Apps-Portals/Odata-feed-and-entity-permissions/td-p/517487
Microsoft | Power Apps
Product
Pricing
Partners
Learn
Support
Community

Odata feed and entity permissions

04-06-2020 06:23 AM

Hi!

I am trying to learn about the odata feed that can be enabled on entity lists. I've got it working and is now wondering about the security. I have read both that **it does use entity permissions** and **that it is open for anonymous access**. When trying it out it is not availiable for anonymous access (according to me). Byt I am still a portal rookie and not really trusting it when the internet occasionally says otherwise.

Regards / lisa

Message 1 of 2 (154 Views)

04-08-2020 06:52 AM

Hello Byla,

I hope you are keeping well. I can confirm that the odata feeds are anonymous and accessible by anyone that can access the portal. They do not need to be signed in and will not need any entity permissions to access the data. https://docs.microsoft.com/en-us/powerapps/maker/portals/configure/entity-lists#entity-list-odata-fe...

I hope this clears things up and I invite you to review the link provided above.

Thanks,

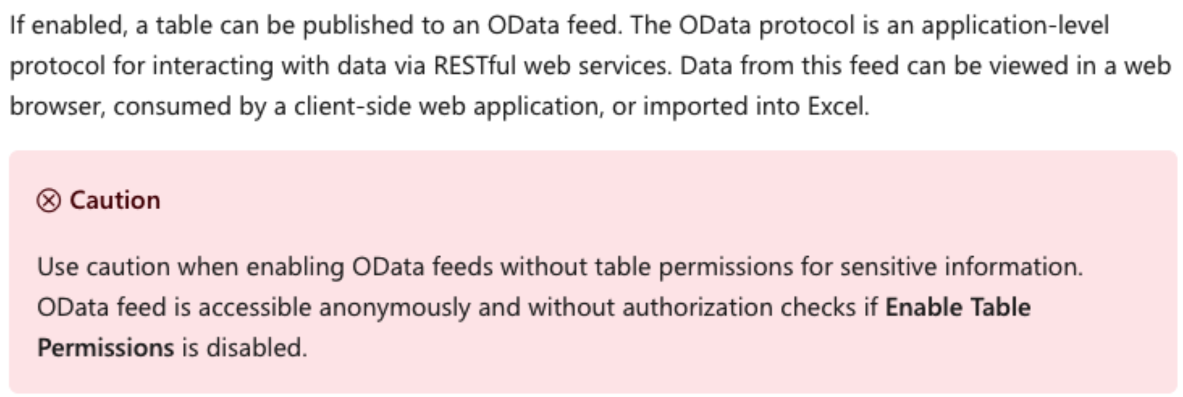
Mark Biggerstaff
Dynamics Support

Confirmation by Microsoft support that OData API feeds can be configured for anonymous access

Background

Microsoft Power Apps are a product for making “low code”, cloud-hosted business intelligence apps. Power Apps portals are a way to create a public website to “give both internal and external users secure access to your data.” Users can create websites in the Power Apps UI with application capabilities like user authentication, forms for users to enter data, data transformation logic, storage of structured data, and APIs to retrieve that data by other applications. Portals provide a public website for interacting with those apps. Typically a business unit or polity uses a portal as an interface with a closely-related audience like customers, sales partners, employees, or citizens.

One of the options for Power Apps is to enable OData (Open Data Protocol) APIs for retrieving data from Power Apps lists, which are the Power Apps configuration used to “expose records for display on portals.” Lists pull data from tables, and limiting access to the list data that a user can see requires enabling Table Permissions. “To secure a list, you must configure Table Permissions for the table for which records are being displayed and also set the Enable Table Permissions Boolean value on the list record to true.” If those configurations are not set and the OData feed is enabled, anonymous users can access list data freely.



If enabled, a table can be published to an OData feed. The OData protocol is an application-level protocol for interacting with data via RESTful web services. Data from this feed can be viewed in a web browser, consumed by a client-side web application, or imported into Excel.

⊗ **Caution**

Use caution when enabling OData feeds without table permissions for sensitive information. OData feed is accessible anonymously and without authorization checks if **Enable Table Permissions** is disabled.

Microsoft’s Power Apps Portals documentation warns that OData feeds are public if misconfigured

Configuration options that allow a product to sometimes be used for data sharing and sometimes be used for storing sensitive data create the potential for data leaks. Power Apps portals have options built in for sharing data, but they also have built in data types that are inherently sensitive. In this case, we found four separate portals with lists called “msemr_appointmentemrset” used for storing information about people setting medical appointments, strongly suggesting this is a schema in the Power Apps catalog rather than one that separate users all came up with.

Power Apps Portals lists are created to display data from tables. These tables are stored within Microsoft Dataverse. When a developer enables the OData feed on the “OData Feed” list settings tab, they must also activate the “Enable Table Permissions” option on the “General” list settings tab unless they wish to make the OData feed public. This is due to all lists having table permissions disabled by default. Table permissions by default will in fact prevent anonymous data access, but lists ignore these permissions and any custom table permissions unless the developer activates table permissions for the list.

At least, that was the state of Power Apps portals in June, 2021. As a result of this research project, Microsoft has since made changes to Power Apps portals such that table permissions are enabled by default. This report documents the steps that led to that change.

Discovery

On May 24 2021, an UpGuard analyst first discovered that the OData API for a Power Apps portal had anonymously accessible list data including personally identifiable information. The owner of that application was notified and the data secured. That case led to the question of whether there were other portals with the same situation– the combination of configurations allowing lists to be accessed anonymously via OData feed APIs, and sensitive data collected and stored by the apps.

First we identified the addresses of Power Apps portals. Power Apps portals are assigned a subdomain of the site "powerappsportals.com," so using common subdomain enumeration techniques generated a list of customer portals. We also discovered two other primary domains used for similar Microsoft products with the same OData configuration options: powerappsportals.us, which appears to be for US governmental use, and microsoftcrmportals.com, which is for a deprecated version of the product line. Because these portals are intended for users to be able to access them over the internet– people are supposed to be able to find these sites easily– they are generally indexed by search engines, which provides another method for finding portals. That said, there may also be portals (or other Microsoft products with similar configuration options) that were not surfaced using these methods and that we are not aware of.

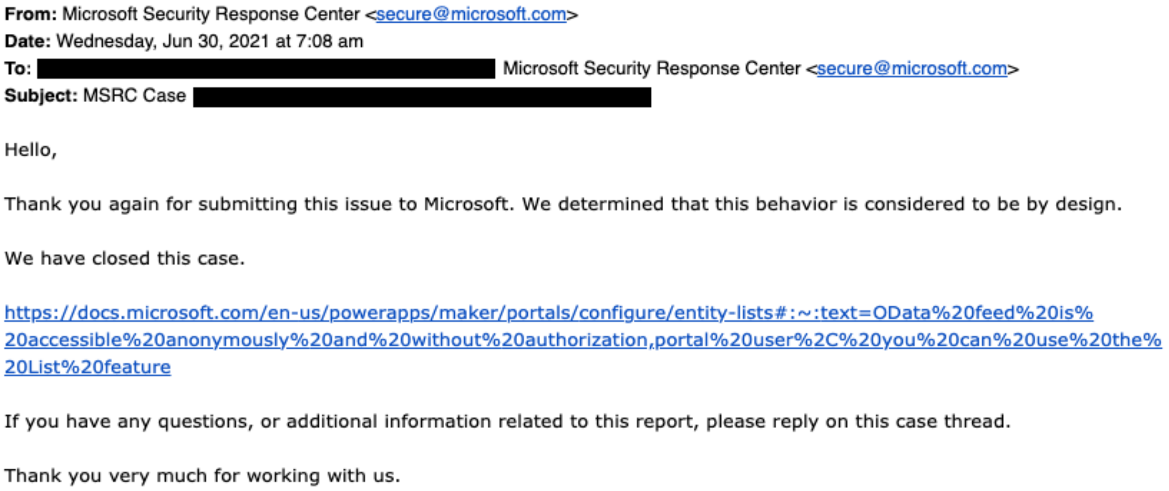
After identifying the addresses for a significant number of portals, we then determined whether any OData lists were publicly accessible for each portal. If OData APIs were enabled, the lists were listed at the `_odata` endpoint. That is, for any given portal, you can determine whether OData lists are enabled by going to example.powerappsportals.com/_odata, and the lists would be displayed in your browser. Visiting the URL for a list would either display the data, if anonymous access was allowed, or show a message that access was forbidden, if some level of table permissions were enabled. The full URL would be something like example.powerappsportals.com/_odata/mylist, making it very easy to go from a list of portals to publicly accessible lists.

Finally, we manually analysed the data to determine sensitivity, which led to the conclusion that there were many Power Apps portals with likely sensitive data. Given the number of portals, the limitations of our discovery methods, and the lack of existing public awareness concerning this issue, we thought the best course would be to disclose our findings as a vulnerability to Microsoft. They would have the technical access and personnel resources to audit all Power Apps portals (and potentially other products in the Power Platform) and notify the owners of those accounts before public disclosure. That seemed like the best possible outcome– all sensitive data secured followed by a public disclosure of the underlying issue– and so this was the first route we pursued.

Vulnerability disclosure to Microsoft

On Thursday, June 24, 2021, we submitted a vulnerability report to the Microsoft Security Resource Center. The report included the steps to identify OData feeds that allowed anonymous access to list data and URLs for accounts that were exposing sensitive data. Among the examples of sensitive data exposed via OData APIs were three Power Apps portals used by American governmental entities to track COVID-19 tracing or vaccination and a portal with job applicant data including Social Security Numbers. We mentioned that these instances were examples of a broader pattern, with a significant number of Power Apps portals configured to allow anonymous access to lists and exposing PII as a result. The case was accepted by the automated MSRC process and a Microsoft analyst began investigating that day.

Over the next day we corresponded with the Microsoft analyst to clarify steps to reproduce and Microsoft's relationship to the powerappsportals.com domain. On Tuesday June 29, the case was closed, and the Microsoft analyst informed us that they had "determined that this behavior is considered to be by design."



From: Microsoft Security Response Center <secure@microsoft.com>
Date: Wednesday, Jun 30, 2021 at 7:08 am
To: [redacted] Microsoft Security Response Center <secure@microsoft.com>
Subject: MSRC Case [redacted]

Hello,

Thank you again for submitting this issue to Microsoft. We determined that this behavior is considered to be by design.

We have closed this case.

https://docs.microsoft.com/en-us/powerapps/maker/portals/configure/entity-lists#:~:text=OData%20feed%20is%20accessible%20anonymously%20and%20without%20authorization,portal%20user%2C%20you%20can%20use%20the%20List%20feature

If you have any questions, or additional information related to this report, please reply on this case thread.

Thank you very much for working with us.

Response from Microsoft Security Response Center

Notification to affected entities

We had discovered over a thousand anonymously accessible lists across a few hundred portals that needed to be analyzed and potentially notified. Ideally, Microsoft would have been involved in doing so, but our attempt to pursue this option thus far had been unsuccessful– though Microsoft would later take action after we had notified some of the most severe exposures. We spent the next few weeks analysing the data for indicators of sensitivity and reaching out to affected organizations. The notification timelines and data classes for some of the most significant exposures are described below to give a sense of the prevalence and impact of this design decision.

American Airlines

UpGuard notified American Airlines on July 2, 2021. By July 6, 2021, the data was secured. Collection "contacts" had 398,890 records which included full names, job titles, phone numbers, and email addresses. Collection "test" had 470,400 records which included full names, job titles, phone numbers, and email addresses.

Denton County, TX

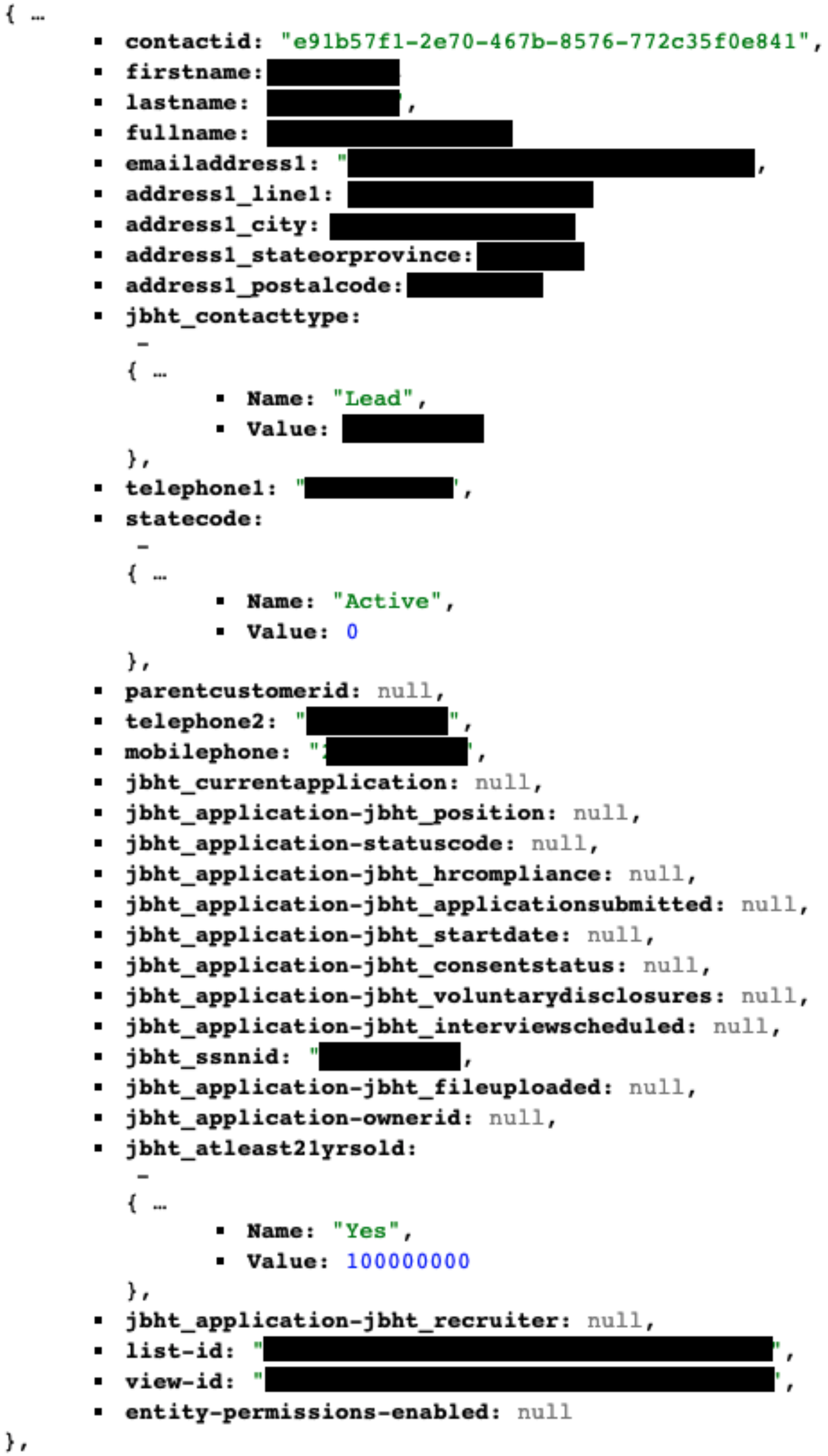
UpGuard sent an email to a Denton County email address related to administering COVID-19 information on July 2. On July 7, an UpGuard analyst called Denton county and spoke with someone who provided the email address for the IT department. The information about the exposed portal was re-sent to that address. The data was secured that day. The significant lists included "msemr_appointmentemrset" which had 632,171 records including vaccination types, appointment dates and times, employee IDs, full names, email addresses, phone numbers, and data of birth. The list "contactVaccinationSet" had 400,091 records with fields for full names and vaccination types, and "contactset" had 253,844 records with full names and email addresses.

Ford

UpGuard notified Ford on July 9, 2021 of an exposure related to their dealer self-service portal. The collections included "systemusers" with 104,578 records, which had fields for full name, title, phone number, and "domainname," which was typically an email addresses. Not all data was present for every record, but 101,895 records had "ford.com" email addresses. Manual analysis confirmed that the job title and name given in some records matched natural persons working for Ford. Other collections described cars being provided to dealerships for use as loaners.

J.B. Hunt

UpGuard notified J.B. Hunt on July 2, 2021. Between July 6 and July 7, 2021 the data was secured. The collection "Contacts" had 905,228 records with fields for full names, email addresses, physical addresses, and phone numbers. 253,288 of these contact records contained data for the field "jbht_ssnid," which was a number matching the format for a US Social Security Number and which contained numbers that have been issued as SSNs. Collection "drugscreen" had 51,028 records containing full names and drug tests dates and locations. The collection "systemusers" had 5,843 containing full names, email addresses, job titles, and phone numbers.



```
{ …
      ▪ contactid: "e91b57f1-2e70-467b-8576-772c35f0e841",
      ▪ firstname: [redacted]
      ▪ lastname: [redacted]',
      ▪ fullname: [redacted]
      ▪ emailaddress1: "[redacted],
      ▪ address1_line1: [redacted]
      ▪ address1_city: [redacted]
      ▪ address1_stateorprovince: [redacted]
      ▪ address1_postalcode: [redacted]
      ▪ jbht_contacttype:
         -
        { …
              ▪ Name: "Lead",
              ▪ Value: [redacted]
        },
      ▪ telephone1: "[redacted]",
      ▪ statecode:
         -
        { …
              ▪ Name: "Active",
              ▪ Value: 0
        },
      ▪ parentcustomerid: null,
      ▪ telephone2: "[redacted]",
      ▪ mobilephone: "[redacted]",
      ▪ jbht_currentapplication: null,
      ▪ jbht_application-jbht_position: null,
      ▪ jbht_application-statuscode: null,
      ▪ jbht_application-jbht_hrcompliance: null,
      ▪ jbht_application-jbht_applicationsubmitted: null,
      ▪ jbht_application-jbht_startdate: null,
      ▪ jbht_application-jbht_consentstatus: null,
      ▪ jbht_application-jbht_voluntarydisclosures: null,
      ▪ jbht_application-jbht_interviewscheduled: null,
      ▪ jbht_ssnnid: "[redacted],
      ▪ jbht_application-jbht_fileuploaded: null,
      ▪ jbht_application-ownerid: null,
      ▪ jbht_atleast21yrsold:
         -
        { …
              ▪ Name: "Yes",
              ▪ Value: 100000000
        },
      ▪ jbht_application-jbht_recruiter: null,
      ▪ list-id: "[redacted]",
      ▪ view-id: "[redacted]",
      ▪ entity-permissions-enabled: null
},
```

Example record from J.B. Hunt collection. Values for “jbht_ssnid” could be verified as actually issued SSNs

Maryland Department of Health

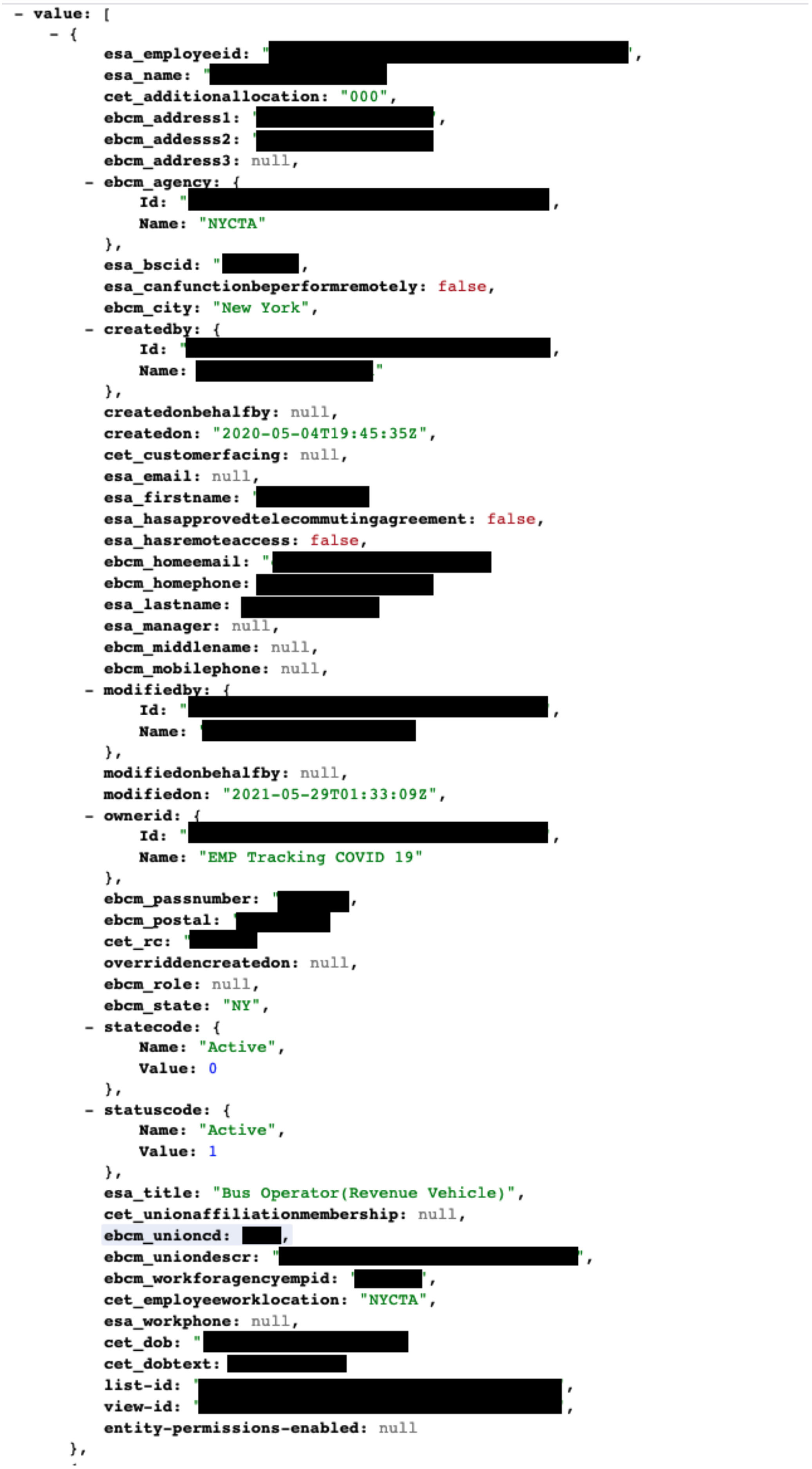
UpGuard notified the Maryland Department of Health on Friday, July 2, 2021. By July 6, 2021, the data was secured. Two lists contained personal information. List “msemr_appointmentemrset” had 280,410 records and included what appeared to be Covid-19 testing appointments containing the appointment date, time, and location, as well as the reference ID of the contact associated with the appointment. List “contactset” had 108,102 records with full names, email addresses, and in some cases phone numbers.

New York City Municipal Transportation Authority and NYC Schools

UpGuard submitted a notification through the MTA’s complaint form, per the link to email their Internet Privacy Compliance Officer on their Privacy Policy, on July 2. The automated response to that form stated it can take up to fifteen days to receive a response. On Friday, July 9 an UpGuard analyst called the publicly listed phone number for the MTA Corporate Office. After speaking with a person at the help desk, the call was directed to Business Services, so the analyst found an email address for MTA Business Services on a public website and sent an email notification to them. Later in the day on July 9, we received a response to the original submission saying they had forwarded it to Threat Intelligence. On Monday, July 12 the data was still available, so we sent notification to the Office of Information Technology Services for the State of New York. On Thursday July 15, an analyst spoke on the phone with an employee at the NYC Department of Information Technology whose contact information had been provided by a mutual friend. The DOIT employee provided the email address for the NYC security operations center, and email notification was sent to that address. The exposed data was secured by the next day.

An exposure for NYC Schools had a similar notification arc. Email notification was first sent on July 9 to a public email address for NYC Schools. UpGuard sent another email to a different address related to NYC Schools on July 12. The notification to the State of New York Office of Information Technology Services on July 12 also included the location of the NYC Schools exposure. Like with the MTA exposure, it was closed within a day of the email to the NYC SOC.

The MTA portal had lists called “EmployeeEsa” with 78,865 records containing full names, DoB, email addresses, phone numbers, union membership, and work locations. “VaccinatedEmployees” with 63,706 records containing full names, vaccination dates, and vaccination types. Another list, “VaccineIntakes”, held 52,253 records containing full names, DoB, email addresses, phone numbers, and physical addresses.



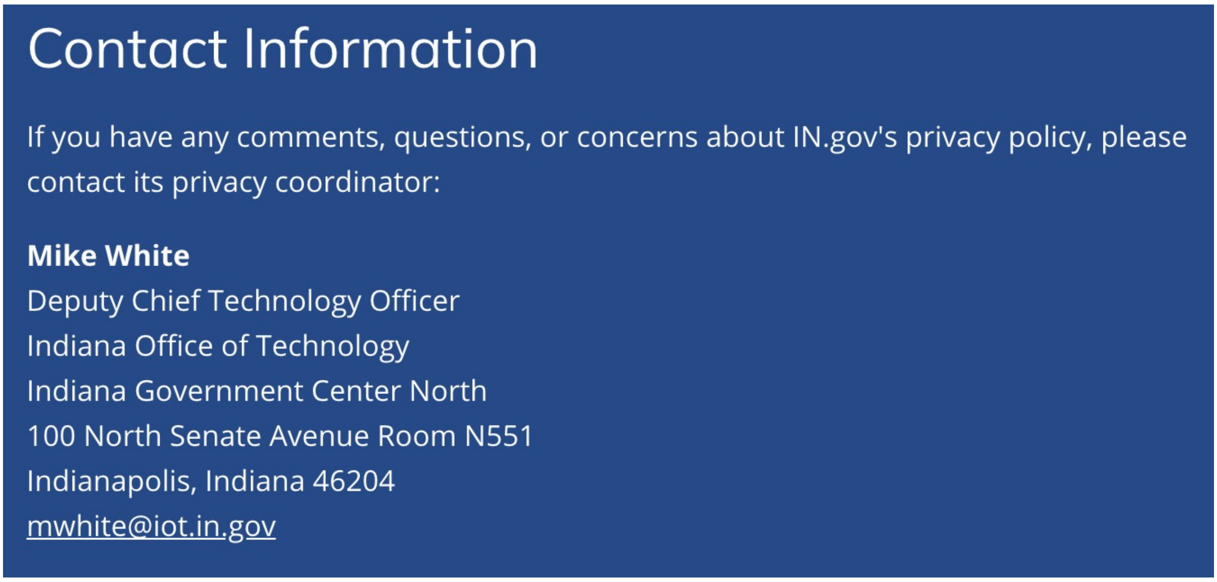
```
- value: [
  - {
        esa_employeeid: "[redacted]",
        esa_name: "[redacted]
        cet_additionallocation: "000",
        ebcm_address1: "[redacted]",
        ebcm_addesss2: "[redacted]
        ebcm_address3: null,
      - ebcm_agency: {
            Id: "[redacted],
            Name: "NYCTA"
        },
        esa_bscid: "[redacted],
        esa_canfunctionbeperformremotely: false,
        ebcm_city: "New York",
      - createdby: {
            Id: "[redacted],
            Name: [redacted]"
        },
        createdonbehalfby: null,
        createdon: "2020-05-04T19:45:35Z",
        cet_customerfacing: null,
        esa_email: null,
        esa_firstname: "[redacted]
        esa_hasapprovedtelecommutingagreement: false,
        esa_hasremoteaccess: false,
        ebcm_homeemail: "[redacted]
        ebcm_homephone: [redacted]
        esa_lastname: [redacted]
        esa_manager: null,
        ebcm_middlename: null,
        ebcm_mobilephone: null,
      - modifiedby: {
            Id: "[redacted],
            Name: "[redacted]
        },
        modifiedonbehalfby: null,
        modifiedon: "2021-05-29T01:33:09Z",
      - ownerid: {
            Id: "[redacted],
            Name: "EMP Tracking COVID 19"
        },
        ebcm_passnumber: "[redacted],
        ebcm_postal: "[redacted]
        cet_rc: "[redacted]
        overriddencreatedon: null,
        ebcm_role: null,
        ebcm_state: "NY",
      - statecode: {
            Name: "Active",
            Value: 0
        },
      - statuscode: {
            Name: "Active",
            Value: 1
        },
        esa_title: "Bus Operator(Revenue Vehicle)",
        cet_unionaffiliationmembership: null,
        ebcm_unioncd: [redacted],
        ebcm_uniondescr: "[redacted]",
        ebcm_workforagencyempid: "[redacted]",
        cet_employeeworklocation: "NYCTA",
        esa_workphone: null,
        cet_dob: "[redacted]
        cet_dobtext: [redacted]
        list-id: "[redacted],
        view-id: "[redacted],
        entity-permissions-enabled: null
    },
```

Example record from New York City MTA collection

The portal belonging to the NYC Department of Education had a list called “contacts” with 412,220 records containing full names and district borough numbers, and a list called “Studentaccounts” with 291,955 records containing full names, usernames, district borough numbers, and email addresses for the “nycstudents.net” mail domain– likely the school-assigned email addresses for students, though it is difficult to verify the identities of minors with publicly available data.

State of Indiana

Per Indiana’s privacy policy, UpGuard notified their designated “privacy coordinator,” Deputy Chief Technology Officer Mike White, on July 2.



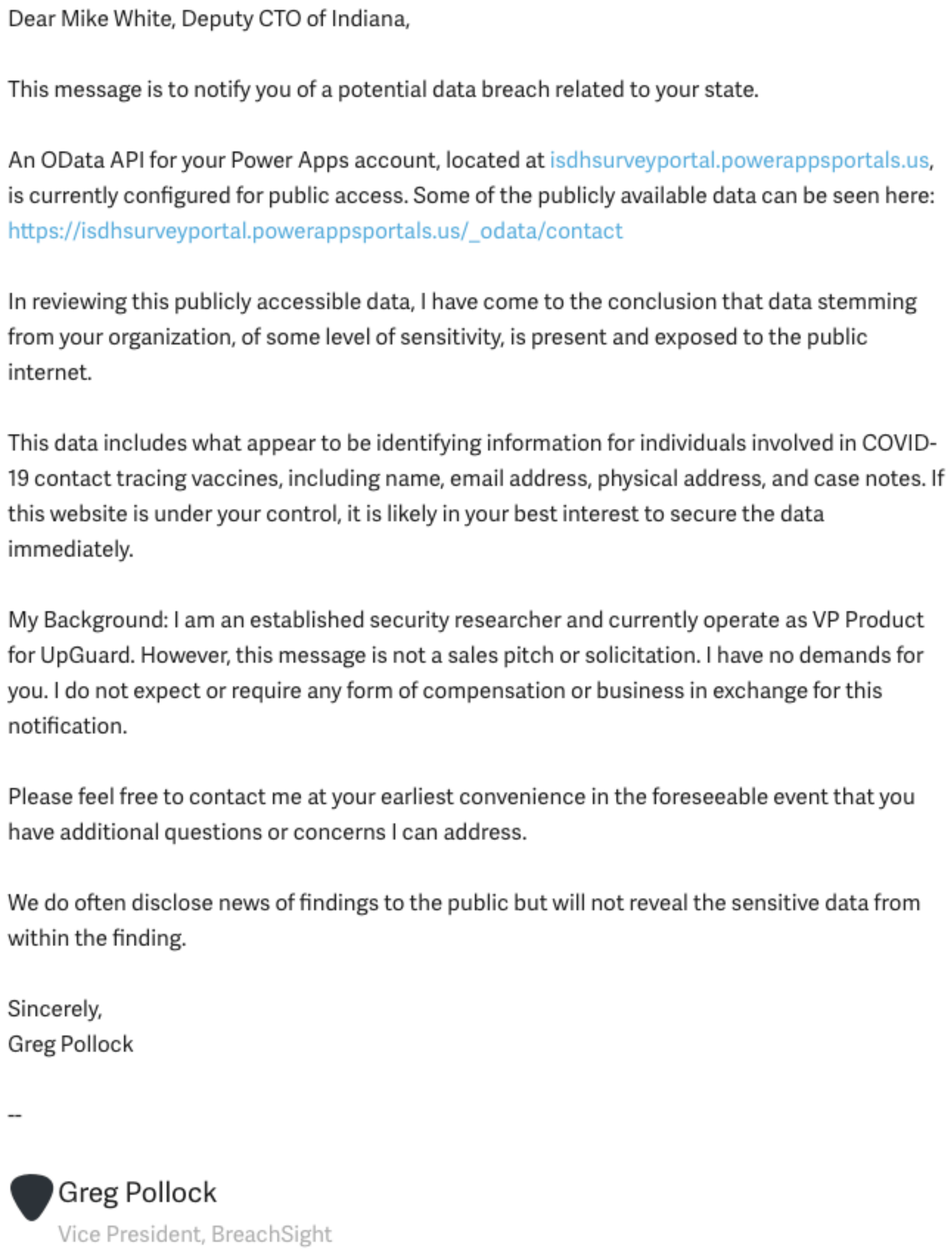
Contact Information

If you have any comments, questions, or concerns about IN.gov's privacy policy, please contact its privacy coordinator:

Mike White
Deputy Chief Technology Officer
Indiana Office of Technology
Indiana Government Center North
100 North Senate Avenue Room N551
Indianapolis, Indiana 46204
mwhite@iot.in.gov

Details of the privacy coordinator for the State of Indiana

The notification email followed the same, standardized template that we use for all data exposure notifications, which has been reviewed by our attorneys at Fenwick and West and approved by the UpGuard board. This notification includes the information that the recipient needs to understand the location of the data, establish its relevance to them, understand why it is sensitive, and confirm that the data is publicly accessible. It also includes the clear statement that the notification is not a sales pitch or solicitation, and no compensation is expected.



Dear Mike White, Deputy CTO of Indiana,

This message is to notify you of a potential data breach related to your state.

An OData API for your Power Apps account, located at isdhsurveyportal.powerappsportals.us, is currently configured for public access. Some of the publicly available data can be seen here: https://isdhsurveyportal.powerappsportals.us/_odata/contact

In reviewing this publicly accessible data, I have come to the conclusion that data stemming from your organization, of some level of sensitivity, is present and exposed to the public internet.

This data includes what appear to be identifying information for individuals involved in COVID-19 contact tracing vaccines, including name, email address, physical address, and case notes. If this website is under your control, it is likely in your best interest to secure the data immediately.

My Background: I am an established security researcher and currently operate as VP Product for UpGuard. However, this message is not a sales pitch or solicitation. I have no demands for you. I do not expect or require any form of compensation or business in exchange for this notification.

Please feel free to contact me at your earliest convenience in the foreseeable event that you have additional questions or concerns I can address.

We do often disclose news of findings to the public but will not reveal the sensitive data from within the finding.

Sincerely,
Greg Pollock

--

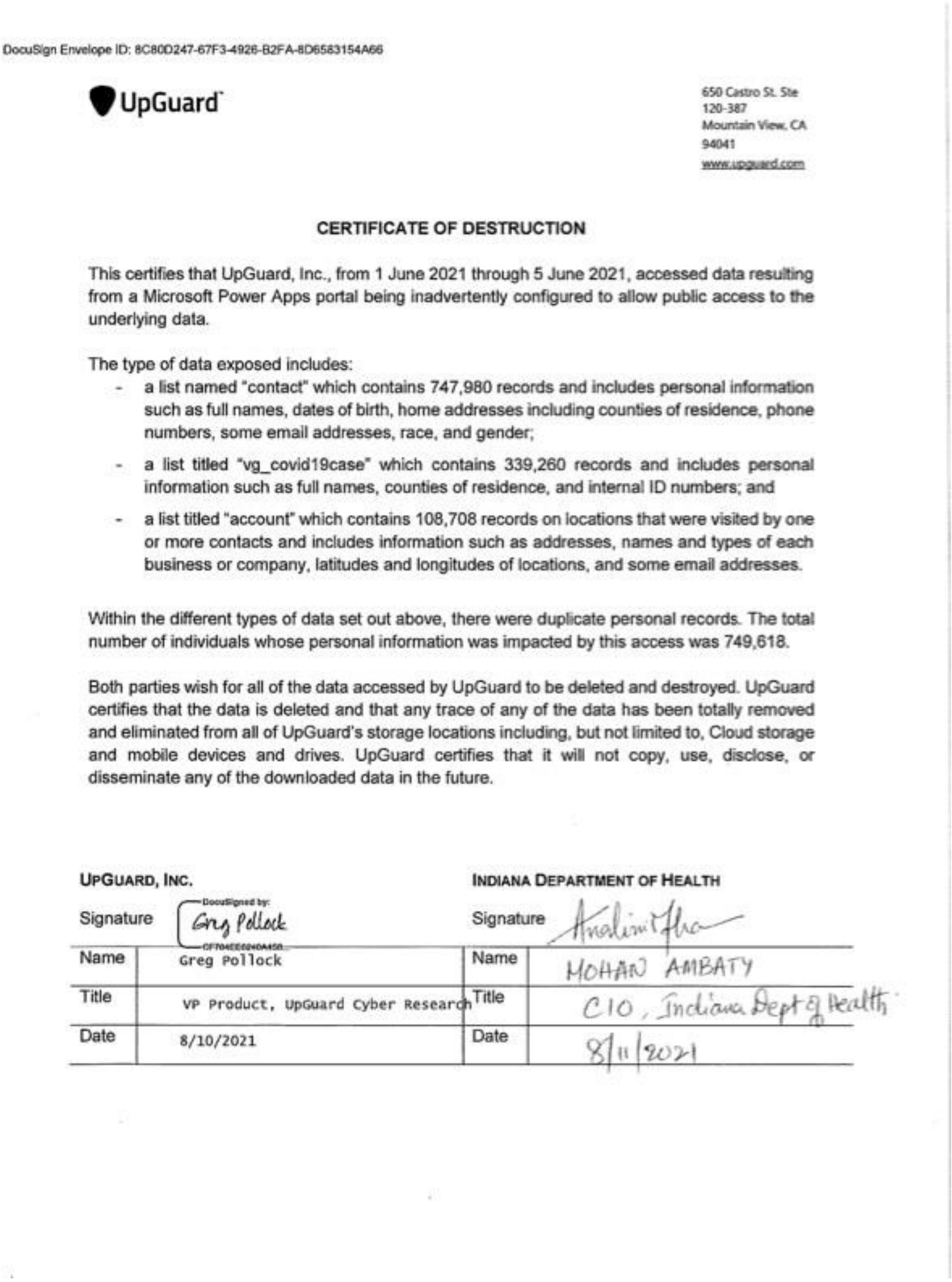
Greg Pollock
Vice President, BreachSight

Notification email sent by UpGuard researcher to the State of Indiana's privacy coordinator

Public access to the data was removed between July 6 and July 7. On July 12, a member of the Indiana Department of Health responded and we began coordinating on the steps toward data deletion, which ultimately led to a conference call on August 2 with several members of the Indiana Department of Health (INDOH), including the Privacy Officer and CIO, and UpGuard’s VP of Product and General Counsel. During that call Indiana requested a copy of the data UpGuard had been able to download in order to confirm what data had been anonymously accessible. Because Power Apps was software as a service managed by Microsoft, the end users did not have direct access to logs needed to audit access, making a data replica particularly necessary. From conversations with personnel in Indiana and elsewhere, it is UpGuard's understanding that Microsoft has provided logs to customers upon request so that they can audit access for reported cases of data exposure.

On August 3 UpGuard and INDOH personnel worked together to securely transfer a replica of the datasets to Indiana's SFTP server, as well as confirming that another collection named "vg_covid19interview" had been configured to deny anonymous access, and thus was not part of the data UpGuard downloaded. UpGuard also clarified when the download occurred. As late as August 6, the INDOH team did not know when the data had been downloaded, though the logs they obtained from Microsoft ultimately allowed them to confirm that no other parties had accessed the data.

By August 11, both parties signed a declaration certifying the facts about the exposure. These facts are that the data was publicly exposed, the number of individuals affected, the types of data exposed, and that UpGuard had destroyed its copy of the data. The certificate of destruction was returned to UpGuard by the Privacy Officer of the Indiana DOH and signed by the CIO of the Indiana DOH.



DocuSign Envelope ID: 8C80D247-67F3-4926-B2FA-8D6583154A66

UpGuard

650 Castro St. Ste
120-387
Mountain View, CA
94041
www.upguard.com

CERTIFICATE OF DESTRUCTION

This certifies that UpGuard, Inc., from 1 June 2021 through 5 June 2021, accessed data resulting from a Microsoft Power Apps portal being inadvertently configured to allow public access to the underlying data.

The type of data exposed includes:

- a list named "contact" which contains 747,980 records and includes personal information such as full names, dates of birth, home addresses including counties of residence, phone numbers, some email addresses, race, and gender;
- a list titled "vg_covid19case" which contains 339,260 records and includes personal information such as full names, counties of residence, and internal ID numbers; and
- a list titled "account" which contains 108,708 records on locations that were visited by one or more contacts and includes information such as addresses, names and types of each business or company, latitudes and longitudes of locations, and some email addresses.

Within the different types of data set out above, there were duplicate personal records. The total number of individuals whose personal information was impacted by this access was 749,618.

Both parties wish for all of the data accessed by UpGuard to be deleted and destroyed. UpGuard certifies that the data is deleted and that any trace of any of the data has been totally removed and eliminated from all of UpGuard's storage locations including, but not limited to, Cloud storage and mobile devices and drives. UpGuard certifies that it will not copy, use, disclose, or disseminate any of the downloaded data in the future.

UPGUARD, INC.		INDIANA DEPARTMENT OF HEALTH	
Signature	DocuSigned by: Greg Pollock	Signature	
Name	Greg Pollock	Name	MOHAN AMBATY
Title	VP Product, UpGuard Cyber Research	Title	CIO, Indiana Dept of Health
Date	8/10/2021	Date	8/11/2021

Certificate of destruction co-signed by UpGuard and the State of Indiana, confirming that Indiana misconfigured their Power Apps portal to allow public access to the underlying data

In one portal, the list "contact" had 747,980 records and the list "vg_covid19case" had 339,260. Between them, 749,618 individuals' data was impacted. Another portal had a similar schema but much smaller quantities of data, and may have been an earlier iteration of the same functional site. The data in "vg_covid19case" included full names, county, date of birth. The list "contact" had full names, date of birth, some email addresses, home address, and phone number.

On August 10, INDOH requested that UpGuard wait until at least August 20 before publishing any report while they completed their response process. Out of respect for the privacy of the individuals whose data was impacted, UpGuard complied with the timeline requested by INDOH.

On August 17, the State of Indiana issued a press release announcing this exposure and saying it would be notifying affected persons. The press release also included several misrepresentations about the nature of UpGuard's actions. UpGuard's Director of PR repeatedly attempted to reach Indiana's designated media contact by phone in order to make them aware of how to correct those misrepresentations but received no response.

The most significant of those misrepresentations are that UpGuard "improperly accessed" the data and that UpGuard performed this action to seek business from Indiana. As the attestation signed from the INDOH CIO shows, the system was misconfigured by the State of Indiana such that anonymous users were authorized to access the data. UpGuard did not exceed our authorized access, and while the data should not have been public, the nature of the data could only be ascertained by downloading and analyzing it.

Second, there is no evidence to support the statement by Tracy Barnes, CIO for the state of Indiana, that UpGuard "intentionally looks for software vulnerabilities, then reaches out to seek business." UpGuard's notification email explicitly states the non-commercial nature of the notification. The conference call with the INDOH team and UpGuard was recorded by INDOH, and if Mr. Barnes wishes to release it, the recording will show that all questions about UpGuard's commercial offerings were addressed only insomuch as to say we could not discuss commercial relations with an entity we have notified of a breach. The same goes for all email communication between UpGuard and Indiana. During five years of sending data breach notifications, UpGuard has never approached Indiana or any other company notified of a breach for business, and there is no merit to Mr. Barnes' statement. On the contrary, UpGuard has provided hours of unremunerated support in service of Indiana Department of Health and the people it serves.

Abuse report to Microsoft

During our initial canvass of Power Apps portals we discovered a few for groups at Microsoft. Analyzing those portals, however, led to the discovery on July 6 of the deprecated microsoftcrmportals.com domain. This domain had more apps created by Microsoft groups, some with very large collections of data. By July 9 we had completed some analysis of the accounts across the three domains and determined which were for Microsoft groups.

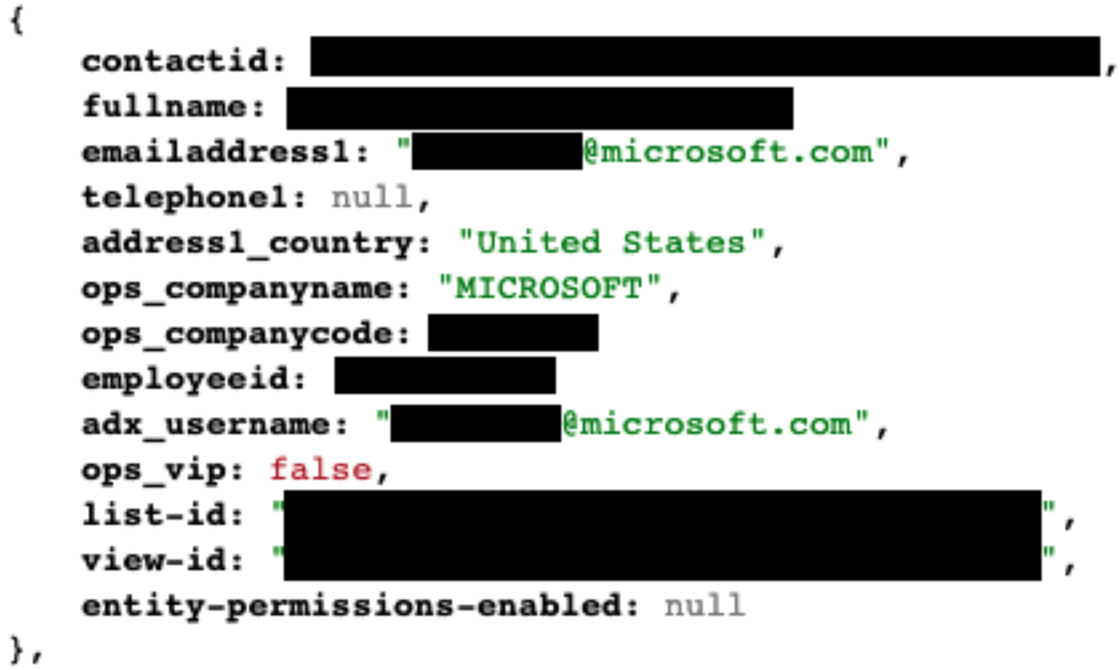
We replied to the original email thread with the MSRC, thinking that would be the quickest way to get it in front of an analyst who could route it to the correct recipient. After no response, we opened a new case in the MSRC on July 13 and were informed on July 14 that we needed to submit an abuse report instead. On July 15 we submitted an abuse report with a list of all Power Apps and Microsoft CRM accounts we knew of that had Microsoft data. By Friday, July 16, the most serious exposure (a collection of 332,000 email addresses and employee IDs used for Microsoft's global payroll services) was no longer public. By the following Monday, July 19, all but one of the remaining portals that were exposing personally identifiable information had removed public access for lists.

The one portal not yet secured on that day was for the administration of selling Azure China through 21Vianet. On July 20 we sent notification to 21Vianet by an email address listed on their website. On July 22 we sent another notification to an @microsoft.com email address listed on the support page for the portal. Within an hour a contractor working for Microsoft– their email domain was microsoft.com but their signature identified them as working for another company– had responded and the data was secured soon after.

Significant Microsoft portals

Global Payroll Services

The Global Payroll Services Portal was a site for handling payroll questions from Microsoft's global workforce, deprecated as of October 2020, when it was migrated to a newer version of the software. The list "contacts" had 332,000 records of people on the global payroll with their @microsoft.com email address, full name, phone numbers that appear to be for personal use, and employee id, their "ops_company," and whether they are an "ops_vip." The convention for naming a user in their email address also tacitly denotes whether they are a contractor or an employee of Microsoft proper. The list "Cases" had metadata about the employees' questions like the ticket title– examples include "Wrong Salary has been deposited to my account" and "Payslip January 2017 - Clarification on Taxable Amount"– the ticket status, and the name of the person who worked on it.



```
{
    contactid: [redacted],
    fullname: [redacted]
    emailaddress1: "[redacted]@microsoft.com",
    telephone1: null,
    address1_country: "United States",
    ops_companyname: "MICROSOFT",
    ops_companycode: [redacted]
    employeeid: [redacted]
    adx_username: "[redacted]@microsoft.com",
    ops_vip: false,
    list-id: "[redacted]",
    view-id: "[redacted]",
    entity-permissions-enabled: null
},
```

Example record for Microsoft Global Payroll Services collection

Business Tools Support

There were two portals related to Business Tools Support. One had a list "Contact" with 45,810 records, with data including users' full names and users' @microsoft.com email addresses. Other lists in this portal included "Incidents" and "CasesSharedToContacts" that described service tickets. The other portal had the same lists and appeared to be an older version of the same site.

Customer Insights Portal

A portal to “manage customer engagements and programs” had the list “Contacts” with 277,400 records that included full name and business email address. Many but not all of the email addresses were for the microsoft.com mail domain. The others were email addresses for users that could be identified as natural persons given their name and their employer’s mail domain. Other lists described what programs the contacts were involved in.

Mixed Reality

Three portals related to Mixed Reality had similar lists. The most significant list was “contacts,” which contained 39,210 records for primarily non-Microsoft users, some of which had business email accounts and some of which were from personal email providers like Gmail or universities. The data present was the user’s full name, email address, and the name of their Microsoft liaison.

Azure China

Many U.S. tech companies sell their products in China through resellers, and Azure China is the same. From Microsoft’s documentation: “Microsoft Azure operated by 21Vianet (Azure China) is a physically separated instance of cloud services located in China. It's independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd..” This portal, which had a Microsoft logo and a link to the Microsoft privacy policy in the footer, appeared to be the partner interface for managing the agreements between Microsoft and 21Vianet. There were several lists for the identities involved in different roles, with 1,264 entries in “AllContacts” with full name, role, and email address. The list “AllAgreements” had 7,936 entries, each of which described an agreement with the customer company name and the people involved in executing it. Some of the agreement metadata indicated they had been last modified as recently as June of 2021.

Microsoft Response

The process of notifying affected entities has resulted in ongoing conversations and visibility into Microsoft’s extended response. From those conversations we learned that Microsoft eventually did take follow up actions. At some point, Microsoft notified government cloud customers of this issue. We did not receive that notification, of course, but could observe its effect in that several lists for portals on powerappsportals.us that had been public in June were no longer public by the end of July.

Additionally, Microsoft has released a tool for checking Power Apps portals and planned changes to the product so that table permissions will be enforced by default. To diagnose configuration issues, the Portal Checker can be used to detect lists that allow anonymous access. More importantly, newly created Power Apps portals will have table permissions enabled by default. Tables configurations can still be changed to allow for anonymous access, but defaulting to permissions enabled will greatly reduce the risk of future misconfiguration.

Conclusion

For several months the UpGuard Research team has worked to navigate a way toward the best resolution of Power Apps portals exposing personal data. We have now reached the end of that journey, and if we haven't reached the best conclusion possible, we can at least comment on what we have learned.

While we understand (and agree with) Microsoft's position that the issue here is not strictly a software vulnerability, it is a platform issue that requires code changes to the product, and thus should go in the same workstream as vulnerabilities. It is a better resolution to change the product in response to observed user behaviors than to label systemic loss of data confidentiality an end user misconfiguration, allowing the problem to persist and exposing end users to the cybersecurity risk of a data breach. Ultimately, Microsoft has done the best thing they can, which is to enable table permissions by default and provided tooling to help Power Apps users self-diagnose their portals. One potential learning for platform operators is to take ownership of misconfiguration issues sooner, rather than leave third-party researchers to identify and notify all instances of such misconfigurations.

Another improvement for software as a service operators like Microsoft is to improve end user visibility of access logs. Software as a service is convenient because it removes the need to administer the underlying infrastructure, but certain information from that infrastructure– most notably access logs– is crucial to executing incident response plans.

For anyone who digitally processes sensitive information– that is, virtually all companies and government bodies– being prepared for a notification of a data leak or other incident will improve outcomes. In some cases, we struggled to get in contact with anyone who would remediate the issue. Providing a designated privacy contact on an easily searchable web page improves that part of the response process. Further, it must be an email address rather than a form. Researchers sometimes need evidence of their exact message to affected entities in order to refute baseless smears, and email messages provide a useful record for those cases.

Finally, technology leaders should have a general understanding of the phenomenon of data exposures. As more information is moved online, the frequency of sensitive data being made publicly available increases. It is and always has been legal to view public information, and the U.S. Supreme Court has solidified the basis for security researchers to work on information that allows anonymous access in *Van Buren v. United States*. Efforts to malign researchers cannot undo mistakes of the past, but they can deter those who would help in the future.