38 Million Records Exposed from Microsoft Power Apps of Dozens of Organisations

August 24, 2021 Ravie Lakshmanan

(https://thehackernews.com/images/-ZcGq0R8ecJ8/YSTAvmTgkmI/AAAAAAAADnc/HwwQbTEDYysOOp8y7ltgDqCM5iw3pz6QwCLcBGAsYHQ/s0/microsoft-power-apps.jpg)

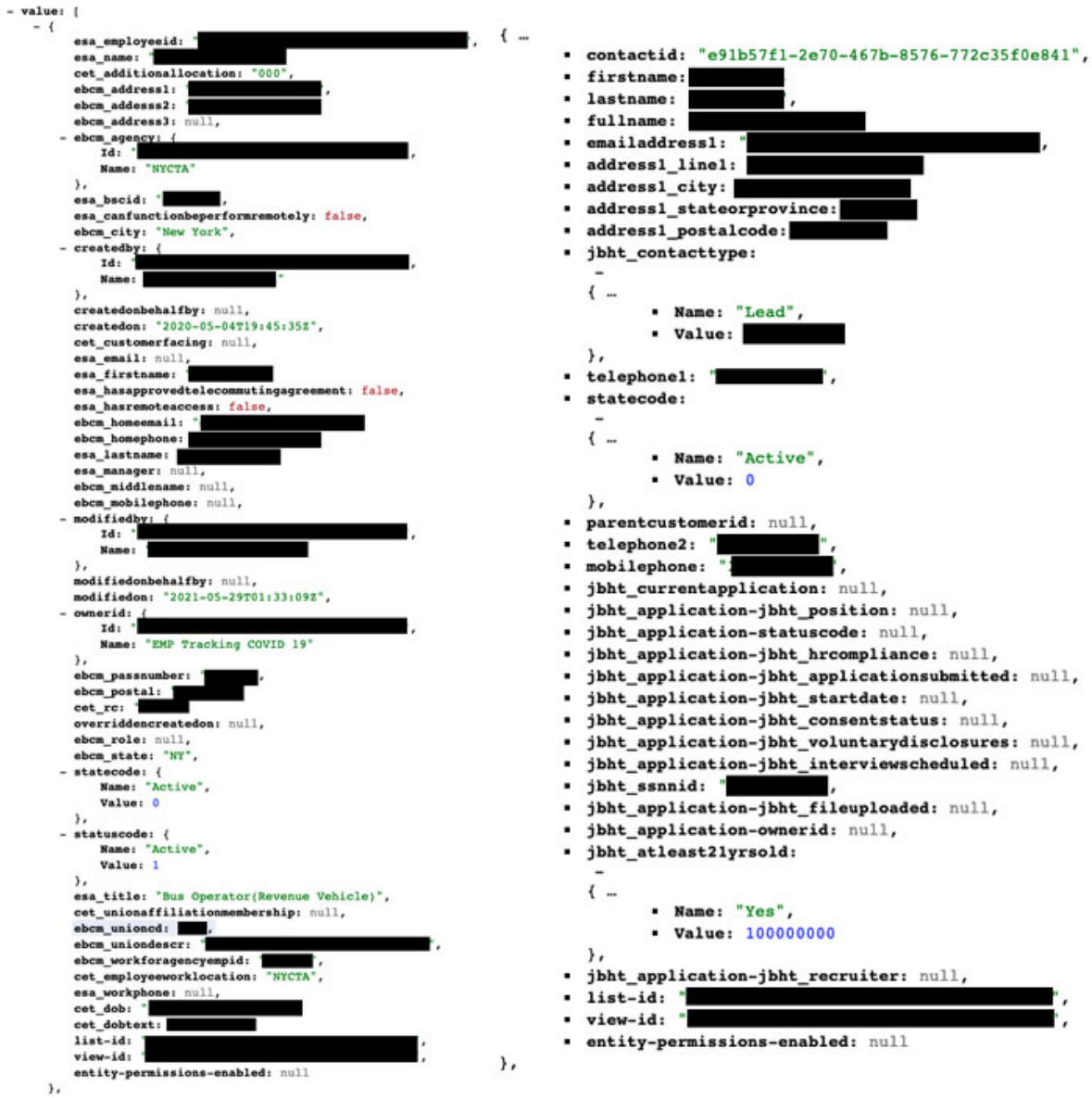
More than 38 million records from 47 different entities that rely on Microsoft's Power Apps portals platform were inadvertently left exposed online, bringing into sharp focus a "new vector of data exposure."

"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 Research team said (https://www.upguard.com/breaches/power-apps) in a disclosure made public on Monday.

Governmental bodies like Indiana, Maryland, and New York City, and private companies such as American Airlines, Ford, J.B. Hunt, and Microsoft are said to have been impacted. Among the most sensitive information that was left in the open were 332,000 email addresses and employee IDs used by Microsoft's own global payroll services, as well as more than 85,000 records related to Business Tools Support and Mixed Reality portals.

Power Apps (https://powerapps.microsoft.com/en-us/) is a Microsoft-powered development platform for building low-code custom business apps that work across mobile and the web using prebuilt templates, in addition to offering APIs to enable access to data by other applications, including options to retrieve and store information. The company describes the service as a "suite of apps, services, and connectors, as well as a data platform, that provides a rapid development environment to build custom apps for your business needs."

But a misconfiguration in the way a portal could share and store data could lead to a scenario wherein sensitive data is made publicly accessible, resulting in a potential data leak.



(https://thehackernews.com/images/-xLk9siWH1qY/YSS9cpE55FI/AAAAAAAADnU/VF_lyVIFOzYgvFw5lDHLmV1E7Joul2hMwCLcBGAsYHQ/s0/data-leak.jpg)

"Power Apps portals have options built in for sharing data, but they also have built in data types that are inherently sensitive," the researchers said. "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."

UpGuard said it notified Microsoft of the data leakage in June 24, 2021, only for the company to initially close the case, citing the behavior was "by design" but subsequently take actions to alert its government cloud customers of the issue in the wake of an abuse report filed by the security firm on July 15.

(https://go.thn.li/privileged_728)

Additionally, Microsoft has released a tool called Portal Checker (https://docs.microsoft.com/en-us/powerapps/maker/portals/admin/portal-checker-analysis) to diagnose any potential exposure arising out of misconfiguration reasons and has made updates (https://docs.microsoft.com/en-us/powerapps/maker/portals/important-changes-deprecations#table-permission-changes-for-forms-and-lists-on-new-portals) so that "newly created portals will have table permissions enforced for all forms and lists irrespective of the Enable Table Permissions setting."

"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," the researchers noted.

"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."

Found this article interesting? Follow THN on Facebook (https://www.facebook.com/thehackernews) , Twitter (https://twitter.com/thehackersnews) and LinkedIn (https://www.linkedin.com/company/thehackernews/) to read more exclusive content we post.