McDonald's leaks password for Monopoly VIP database to winners

By **Lawrence Abrams (https://www.bleepingcomputer.com/author/lawrence-abrams/)** September 7, 2021 10:56 AM **1**

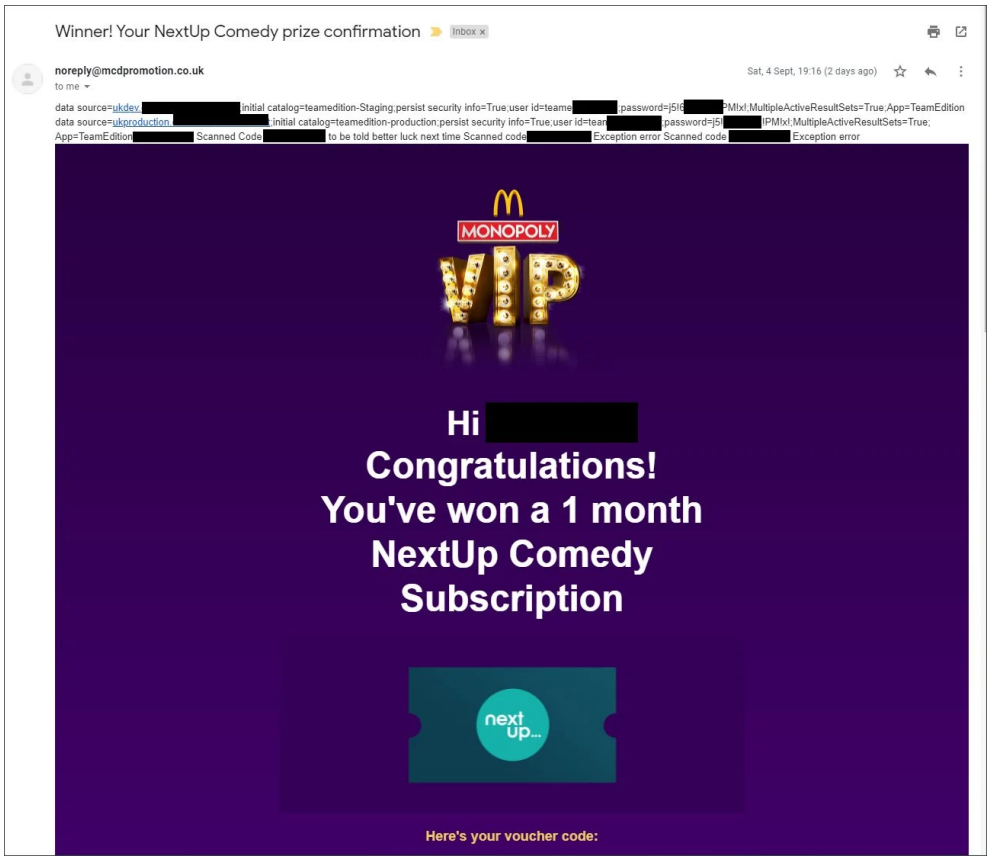
A bug in the McDonald's Monopoly VIP game in the United Kingdom caused the login names and passwords for the game's database to be sent to all winners.

After skipping a year due to COVID-19, McDonald's UK launched their popular Monopoly VIP game on August 25th, where customers can enter codes found on purchase food items for a chance to win a prize. These prizes include £100,000 in cash, an Ibiza villa or UK getaway holiday, Lay-Z Spa hot tubs, and more.

Unfortunately, the game hit a snag over the weekend after a bug caused the user name and passwords for both the production and staging database servers to be in prize redemption emails sent to prize winners.

An unredacted screenshot of the email sent to prize winners was shared with BleepingComputer by Troy Hunt (https://twitter.com/troyhunt) that shows an exception error, including sensitive information for the web application.

This information included hostnames for Azure SQL databases and the databases' login names and passwords, as displayed in the redacted email below sent to a Monopoly VIP winner.



McDonald's Monopoly VIP prize email with database credentials

The prize winner who shared the email with Troy Hunt said that the production server was firewalled off but that they could access the staging server using the included credentials.

"I tried to connect to production to gauge the severity of the issue and whether or not getting in touch was an urgent matter but luckily for them they had a set of firewall rules setup," the person told Troy Hunt in an email shared with BleepingComputer.

"I did however gain access to staging, which I disconnected from immediately for obvious reasons."

As these databases may have contained winning prize codes, it could have allowed an unscrupulous person to download unused game codes to claim the prizes.

Luckily for McDonald's, the person responsibly disclosed the issue with McDonald's, and while they did not receive a response, they later found that the staging server's password was soon changed.

Unfortunately, this was not an isolated issue, as other users reported seeing the credentials and went as far as sharing their experience in a TikTok video (https://www.tiktok.com/@creatorsphereco/video/7004526492055014661).

While the error clearly stated that both a production and staging server's credentials were leaked, McDonald's told BleepingComputer that it was only the staging server that was exposed.

"Due to an administrative error, a small number of customers received details for a staging website by email. No personal details were compromised or shared with other parties," McDonald's told BleepingComputer in a statement.

"Those affected will be contacted to reassure them that this was a human error and that their information remains safe. We take data privacy very seriously and apologise for any undue concern this error has caused."

Update 9/7/21 2:15 PM EST: Added statement from McDonalds.

Related Articles:

Microsoft shares guidance on securing Azure Cosmos DB accounts (https://www.bleepingcomputer.com/news/microsoft/microsoft-shares-guidance-on-securing-azure-cosmos-db-accounts/)

Microsoft warns Azure customers of critical Cosmos DB vulnerability (https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-azure-customers-of-critical-cosmos-db-vulnerability/)

AT&T denies data breach after hacker auctions 70 million user database (https://www.bleepingcomputer.com/news/security/atandt-denies-data-breach-after-hacker-auctions-70-million-user-database/)

Hacker claims to steal data of 100 million T-mobile customers (https://www.bleepingcomputer.com/news/security/hacker-claims-to-steal-data-of-100-million-t-mobile-customers/)

Windows 365 exposes Microsoft Azure credentials in plaintext (https://www.bleepingcomputer.com/news/microsoft/windows-365-exposes-microsoft-azure-credentials-in-plaintext/)