# Security Assessment Report

PERFORMED BY: JOHAN SEPP

## Table of contents

# 1. Results and recommendations

## 1.1 Severity ratings

| Severity | Description |
|---|---|
| **High** | Security vulnerabilities that can give an attacker total or partial control over a system or allow access to or manipulation of sensitive data. |
| **Medium** | Security vulnerabilities that can give an attacker access to sensitive data but require special circumstances or social methods to fully succeed. |
| **Low** | Security vulnerabilities can have a negative impact on some aspects of the security or credibility of the system or increase the severity of other vulnerabilities, but which do not directly compromise the system's integrity. |
| **Info.** | Informational findings are observations made during the assessment that could impact some aspects of security but do not classify as security vulnerabilities. |

Table 1: Severity ratings.

## 1.2 Outline of identified vulnerabilities

| Vulnerability | High | Medium | Low | Info |
|---|---|---|---|---|
| ODBC RCE | | X | | |

Table 2: Outline of identified vulnerabilities

# 1.3 Technical description of findings

## 1.3.1 Microsoft ODBC driver for SQL Server Remote Code Execution Vulnerability

- CVE-2023-36785

**Severity:** Medium

**Description**

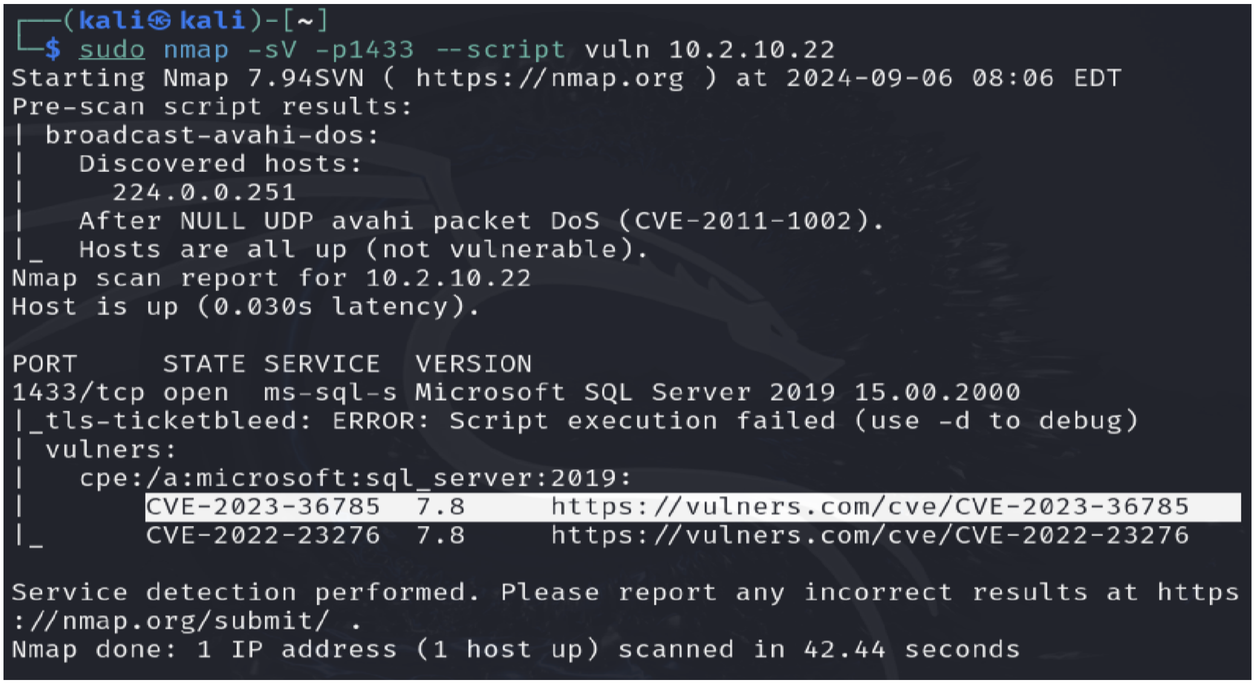
This vulnerability is a remote code execution flaw in the Microsoft ODBC Driver for SQL Server. It allows attackers to execute arbitrary code on the server by exploiting how the driver processes certain SQL commands. The vulnerability specifically stems from a buffer overflow caused by improper handling of SQL Data Access requests. When a specially crafted SQL query is sent, it can trigger this overflow and allow code execution on the affected server.

If the attack is successful, the attacker gains the same privileges as the SQL Server service, potentially leading to full control of the SQL Server and its underlying operating system. This could result in unauthorized access to databases, modification of critical data, exfiltration of sensitive information, or even complete server compromise.

The vulnerable component is not bound to the network stack and the attacker's path is via read/write/execute capabilities. Either: the attacker exploits the vulnerability by accessing the target system locally, remotely, or most commonly the attacker relies on User Interaction by another person to perform actions required to exploit the vulnerability.

Affected hosts:

10.2.10.22:1433, see image 1.
10.2.10.23:1433, see image 2.

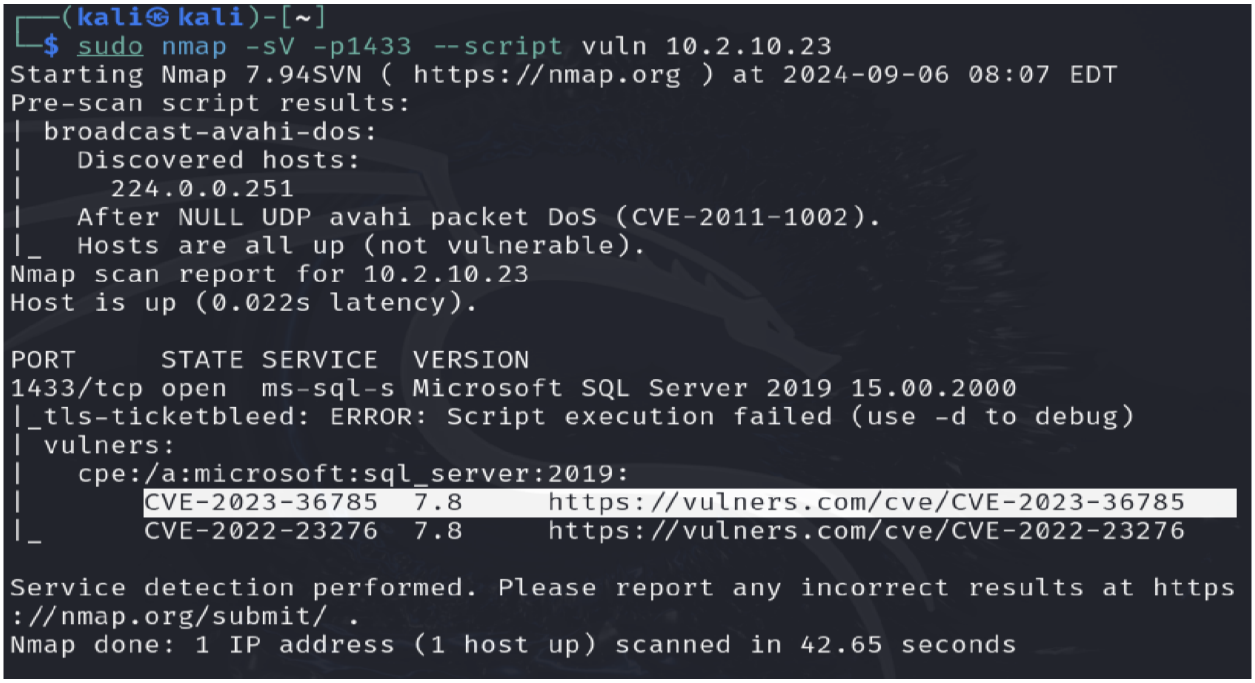


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p1433 --script vuln 10.2.10.22
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 08:06 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.2.10.22
Host is up (0.030s latency).

PORT     STATE SERVICE  VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2019 15.00.2000
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:microsoft:sql_server:2019:
|       CVE-2023-36785  7.8     https://vulners.com/cve/CVE-2023-36785
|_      CVE-2022-23276  7.8     https://vulners.com/cve/CVE-2022-23276

Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.44 seconds
```

Image 1: *"Proof" on host 10.2.10.22*



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -p1433 --script vuln 10.2.10.23
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 08:07 EDT
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for 10.2.10.23
Host is up (0.022s latency).

PORT     STATE SERVICE  VERSION
1433/tcp open  ms-sql-s Microsoft SQL Server 2019 15.00.2000
|_tls-ticketbleed: ERROR: Script execution failed (use -d to debug)
| vulners:
|   cpe:/a:microsoft:sql_server:2019:
|       CVE-2023-36785  7.8     https://vulners.com/cve/CVE-2023-36785
|_      CVE-2022-23276  7.8     https://vulners.com/cve/CVE-2022-23276

Service detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.65 seconds
```

Image 2: *"Proof" on host 10.2.10.23*

**Recommendations**

- Updating your software is the best and most efficient way to mitigate the vulnerability.

- Restrict access to the SQL Server using firewalls, allowing connections only from trusted IP addresses or subnets. This helps to block unauthorized remote access attempts.

- Use host-based firewalls (like Windows Firewall) to limit incoming connections to the server, especially for SQL Server ports like 1433 and 1434.

- Reduce the SQL Server's exposure by limiting the privileges of its service account. This minimizes the damage an attacker could do if the service is compromised.