SQL Server OLE Automation

The security risks involved and advice for SQL Server administrators

Author: Adriaan Vorster, SQL Server DBA @ RadixTrie

Why SQL Server OLE Automation is a Risk

SQL Server OLE Automation is considered a security risk because it allows users to execute arbitrary code outside of the SQL Server environment. This means that an attacker can potentially use this feature to run malicious code or commands on the server, compromising the security and integrity of the system.

OLE Automation enables SQL Server to interact with other applications and components that support the Object Linking and Embedding (OLE) protocol. This feature allows users to execute external scripts or execute commands on the system outside of the SQL Server sandbox. As a result, if an attacker gains access to the SQL Server and has permissions to use OLE Automation, they could use it to execute unauthorised actions such as modifying data, accessing sensitive information, or installing malware on the server.

Advice for SQL Server Administrators

Therefore, SQL Server administrators must carefully manage and limit the use of OLE Automation to only trusted users or applications. They should also keep their servers updated with the latest security patches and ensure that users only have the necessary permissions to access the SQL Server and its features.

References

https://www.imperva.com/blog/how-to-exploit-sql-server-using-ole-automation/

Disclaimer: It is always recommended to log a support request with Oracle Support for any Oracle error you may encounter in your environment.