Vulnerabilities in SQL Server Could Allow Remote Code Execution

Divya T. Aradhya

Write a 1-2 page report identifying at least two vulnerabilities in MS SQL 2008 and describe ways to combat/address those vulnerabilities.

1**. Vulnerabilities in SQL Server Could Allow Remote Code Execution**

What is it? [1]

Microsoft SQL Server 2008 SP3 and SP4, 2008 R2 SP2 and SP3, 2012 SP1 and SP2, and 2014 does not prevent use of uninitialized memory in certain attempts to execute virtual functions, which allows remote authenticated users to execute arbitrary code via a crafted query, aka "SQL Server Remote Code Execution Vulnerability."

Impact:

Confidentiality Impact: Complete (There is total information disclosure, resulting in all system files being revealed.)

Integrity Impact: Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)

Availability Impact: Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)

Access Complexity: Medium (The access conditions are somewhat specialized. Some preconditions must be satisfied to exploit)

Authentication: Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)

Gained Access: None

Vulnerability Type(s): Execute Code

Mitigating Factors: [2]

Requires permissions to create or modify database schema or data

To exploit this vulnerability an attacker would need permissions to create or modify a database.

Workarounds:

Limit permissions on server for database and schema creation

Since the vulnerability is exploitable only within the context of very specific database schema, data, and queries, exploitation can be prevented by strictly controlling who has permissions to create databases and schema on the server. Note that the vulnerability is exposed in very specific edge cases; it is extremely difficult to define the schema and query that would expose the vulnerability.

Additional guidance: In the unlikely event that SQL Server causes an access-violation / data-execution-prevention error during specific query execution, rewrite the query by splitting it into parts and/or adding query hints.

2. **Denial of Service Vulnerability**

What is it? [3]

Microsoft SQL Server 2008 SP3, 2008 R2 SP2, and 2012 SP1 does not properly control use of stack memory for processing of T-SQL batch commands, which allows remote authenticated users to cause a denial of service (daemon hang) via a crafted T-SQL statement, aka "Microsoft SQL Server Stack Overrun Vulnerability."

Impact:

Confidentiality Impact: None (There is no impact to the confidentiality of the system.)

Integrity Impact: None (There is no impact to the integrity of the system)

Availability Impact: Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)

Access Complexity: Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)

Authentication: Single system (The vulnerability requires an attacker to be logged into the system (such as at a command line or via a desktop session or web interface).)

Gained Access: None

Vulnerability Type(s): Denial Of Service

Mitigating Factors: [4]

- In a web-based attack scenario, an attacker could host a specially crafted website that is designed to exploit these vulnerabilities through Internet Explorer, and then convince a user to view the website. The attacker could also take advantage of compromised websites and websites that accept or host user-provided content or advertisements. These websites could contain specially crafted content that could exploit these vulnerabilities. In all cases, however, an attacker would have no way to force users to view the attacker-controlled content. Instead, an attacker would have to convince users to take action, typically by getting them to click a link in an email message or in an Instant Messenger message that takes them to the attacker's website, or by getting them to open an attachment sent through email.
- The XSS Filter in Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 prevents this attack for users when browsing to websites in the Internet Zone. Note that the XSS Filter in Internet Explorer 8, Internet Explorer 9, Internet Explorer 10, and Internet Explorer 11 is enabled by default in the Internet zone, but is not enabled by default in the Intranet Zone.

Workarounds:

Enable Internet Explorer 8 , Internet Explorer 9 , Internet Explorer 10, and Internet Explorer 11 XSS filter for Intranet Zone

You can help protect against exploitation of this vulnerability by changing your settings to enable the XSS filter in the Local intranet security zone. (XSS filter is enabled by default in the Internet security zone.)

References

1. https://www.cvedetails.com/cve/CVE-2015-1763/

2. https://technet.microsoft.com/library/security/ms15-058

3. https://www.cvedetails.com/cve/CVE-2014-4061/

4. https://technet.microsoft.com/library/security/ms14-044