Cyber Security Advisory No. 182 **14-04-2023**

Name: Multiple Vulnerabilities in Microsoft SQL Server

Threat Classification: Remote Code Execution

Affected Services:

- Microsoft SQL Server

Summary:

Three vulnerabilities have been discovered by security researchers and experts in Microsoft SQL Server being used globally, that could allow a remote attacker to execute arbitrary code on the system level. CVE-2023-23384 can be exploited by sending a specially crafted request, while CVE-2023-28304 and CVE-2023-23375 can be exploited by tricking the victim into opening a specially crafted file. CVE-2023-23375 allows an attacker to execute arbitrary code on the system level with SYSTEM privileges.

Severity	**Critical**
Attack Vector	**Network**

Recommendations:

- It is recommended to apply the latest security patches provided by Microsoft for Microsoft SQL Server to mitigate these vulnerabilities
- Implement proper security controls to prevent unauthorized access to Microsoft SQL Server