

Manager's Technical Guide To Microsoft SQL Threats

Threat Assessment

- Exploitation Status: Actively Exploited
- Threat Level: High
- Risk Factors: Exposure of confidential information, Possible arbitrary code execution

Threat Overview

Microsoft SQL Server is a commonly used product to maintain databases and their associated information. The product lends itself to integration with other Microsoft products and Microsoft Windows based networks. It is used in many organizations as the primary database system and occurrences of the product are often deployed on many systems around the enterprise ranging from server systems to workstations. Security vulnerabilities in the Microsoft SQL Server product often expose information kept in these databases and systems, as well as the integrity of administrative control over these devices and the network.

Threat Details:

Two serious threats exist against Microsoft SQL Server installations. The first is a problem with password controls. The database "SA" account is often either not protected by a password or is protected by a simplistic password which is easily guessed. Attackers able to access the database via the "SA" account could have complete access to the database and the system itself. The second issue affecting Microsoft SQL Servers is that several vulnerabilities have been identified in the various versions of the application. Exploit code to perform buffer overflow attacks and other types of input validation attacks against the product have been released. Worms and attackers are commonly exploiting these issues to gain access to the database and the systems hosting the server application. In many cases, the context of the server application is that of a domain administrator, thus giving complete network and device control to the successful attacker exploiting either poor passwords or other SQL vulnerabilities.

Suggested Mitigation:

Administrators of Microsoft SQL Servers need to ensure that all database and system accounts are protected with a strong password (at least 7 characters, alpha-numeric, non-dictionary based). Passwords need to be changed periodically, especially for "SA" and administrator level accounts. Microsoft SQL Server patches, hot fixes and upgrades need to be regularly and consistently applied across the enterprise. Note that the patches for SQL Server need to be applied separately from the operating system patches, but must be maintained on a regular schedule. Where possible, Microsoft SQL Server should be running in the lowest context available, thus limiting the damage a successful attacker can cause.

Further Information and Assistance:

For more information on this or any other type of vulnerability or attacker exploitation, please feel free to contact MicroSolved or one of our SecureAssure™ partners via email or phone. One of our Security Experts will be happy to talk with you about any questions you may have. MSI has specialized in information security assessments, penetration testing, security awareness and data asset protection for more than a decade. Contact us today for all of your information security needs.

