|  |  |
| --- | --- |
| DREAD Score |  |
| Damage Potential | 10 |
| Reproducibility | 10 |
| Exploitability | 10 |
| Affected Users | 10 |
| Discoverability | 10 |
| Total | 50 |

### Summary

Microsoft SQL server comes with a built in System Administrator (SA) account. By default the SA account has full privileges. During the assessment the SA account was found to have a default password of SA or blank. An adversary can use this account to gain administrator level access to the database and can lead to a potential comprise of the system.

### Proof

### Remediation

The default SA account should be disabled. It is recommended to use Windows Authentication. If this is not possible due to business reasons, the SA account should be configured with a strong password. The following guide lines can be used for creating a strong password:

* Use alphanumeric, special characters and spaces
* Use a password that is at least 32 characters long
* Change the password frequently
* Do not reuse previous passwords