Security Advisory: HTTP error codes used for SecQ REST authentication reveal user existence

Date: 11 October 2019

Severity: Low (CVSS 0.1 - 3.9)

Affected versions: all released midPoint versions

Fixed in versions: 4.0.1 (unreleased), 3.9.1 (unreleased), 3.8.1 (unreleased), 3.7.3 (unreleased)

Description

HTTP error codes used for REST authentication based on security questions (a.k.a. SecQ) reveal user existence.

Severity and Impact

Attacker can use REST request to determine whether a user exists. Attacker cannot gain access to any other information or any unauthorized operation.

Mitigation

Users of affected MidPoint versions are advised to upgrade their deployments to the latest builds from the support branches.

As this is a loq severity issue, it is not forcing official maintenance releases of midPoint. However, the fix is provided in all the support branches.

Credit

This issue was reported by Nicolas Destor by the means of EU-Free and Open Source Software Auditing (EU-FOSSA2) project.

See Also

- ~~MID-5725~~ - HTTP error codes used for SecQ REST authentication reveal user existence RESOLVED
- MidPoint page at Hackerone