MyID Product Notification
Microsoft Vulnerability CVE-2020-0601

Introduction

On 14th January 2020, Microsoft reported a security vulnerability in their operating system, reference CVE-2020-0601. This document provides guidance to Intercede customers on the impact of this vulnerability on Intercede products and recommends corrective steps to take to mitigate the vulnerability.

1 What is the impact on MyID?

The affected component (Crypt32.dll) is part of Windows operating systems and is used by MyID for certain cryptographic functions.

1.1.1 Affected Intercede Software

Product/Software Component	Affected?	Reason
MyID Server installations (all versions)	Yes	See information below
MyID Client installations (all versions) *Note- this includes the 'Self Service Request Portal' web page*	Yes	See information below
Mobile apps, including Identity Agent & mobile SDKs	No	Supported mobile operating systems (iOS, Android) are not affected by this vulnerability.

1.1.2 Direct Impacts on MyID

When MyID verifies logon from users that have a smartcard certificate, MyID uses its own copy of the public key stored in its database. This means that even if the certificate used to authenticate leveraged this flaw, it wouldn't enable a logon as MyID is using the public key in its database.

Self Service Request Portal (introduced at MyID v11.4) uses TLS/SSL 2-way authentication to verify the identity of the user. As https connections may be vulnerable, it could be directly affected.

1.1.3 Indirect Impact on Intercede customers

MyID uses the underlying operating system to make https connections (e.g. from client to MyID server, and from MyID server to third party systems (such as Digicert or Primekey EJBCA PKI) – If these endpoints hosted a webserver certificate that leveraged this flaw it could cause the https connection to be trusted where it should not be.

If an administrator installs software on a PC (either a client or a server), then an install that leveraged the flaw to make it appear the software was from publisher A, when in fact it was from publisher B could cause untrusted software (including malware) to be installed on the PC.

MyID relies on other parts of Windows and other Microsoft software (e.g. Internet Information Services, SQL Server) that could be affected by the flaw.

2 What steps should be taken to mitigate the risk on MyID?

It is essential customers follow Microsoft guidance on deploying security updates to their server and computers in use within their environment. Unpatched systems should be considered vulnerable.

3 Will the security updates have any impact on MyID?

Intercede have carried out regression testing of MyID using the operating systems that have been updated with the patches supplied by Microsoft to address the vulnerability. No adverse effects on MyID were found.

Note: Intercede always advise any system changes are first proven in a test environment before being applied to a production system.

4 External References

Please see the following external references for more details about the vulnerability
https://nvd.nist.gov/vuln/detail/CVE-2020-0601
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601