

Scholantis and Heartbleed Security Update

On April 8, 2014, security researchers announced a flaw known as [Heartbleed \(CVE-2014-0160\)](#) which affects the OpenSSL encryption software library used by many websites to protect customers' data. The vulnerability could potentially allow an attacker access to website data and encryption keys.

SharePoint and Scholantis utilize the Windows' implementation of SSL/TLS which is not impacted.

Microsoft has [determined](#) that Microsoft Account, Microsoft Azure, Office 365, Yammer and Skype, along with most Microsoft Services, are not impacted by the Heartbleed vulnerability. Keys and certificates which were only created using OpenSSL tools are also unaffected.

It should be noted that your data and encryption keys could be at risk in other non-Microsoft applications. Developer and cryptography consultant Filippo Valsorda has created [a tool you can use to test websites for the Heartbleed vulnerability](#).

After a review of Scholantis' internal systems we have not identified any vulnerabilities or associated breaches in security.

