BSI

Warnung vor wurmfähiger Schwachstelle

[13.03.2020] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor einer kritischen wurmfähigen Schwachstelle in Windows.

Eine Schwachstelle im Microsoft-Produkt Windows ermöglicht Schadprogrammen neben gezielten Angriffen auch die selbstständige wurmartige Ausbreitung in betroffenen IT-Netzwerken. Das teilt das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit. Da derzeit kein Patch zur Schließung der Sicherheitslücke zur Verfügung stehe, schätzt die Behörde die Lage als kritisch ein. Microsoft hätte bislang nur einen Workaround zur Verfügung stellen können, mit dem die Ausnutzung der Schwachstelle auf SMB-Servern verhindert werden kann. Für einzelne SMB-Clients sei der Workaround nicht geeignet, daher sollte bei betroffenen SMB-Clients eine vollständige Deaktivierung von SMB erwogen werden, so das BSI. Ein ähnliches Szenario hätte 2017 zu den IT-Sicherheitsvorfällen WannaCry und NotPetya geführt.

Bislang keine aktive Ausnutzung bekannt

Dem BSI ist bislang laut eigenen Angaben keine aktive Ausnutzung der Schwachstelle bekannt. Da die Sicherheitslücke jetzt jedoch öffentlich bekannt geworden ist, könnte sich dies kurzfristig ändern. Das BSI rät daher dringend dazu, den von Microsoft beschriebenen Workaround umzusetzen. Außerdem sollte ein Patch, sobald er zur Verfügung steht, kurzfristig eingespielt werden. Zugriffe aus dem Internet auf den von SMB verwendeten Port 445/tcp sollten grundsätzlich von der Firewall geblockt werden Für SMB-Clients der betroffenen Windows-Versionen sollte, bis zur Schließung der Schwachstelle, eine vollständige Deaktivierung von SMB beziehungsweise eine netzwerkseitige Unterbindung geprüft werden. Das BSI hat laut eigenen Angaben eine entsprechende Cyber-Sicherheitswarnung an die Bundesverwaltung, die Betreiber Kritischer Infrastrukturen, die Teilnehmer der Allianz für Cyber-Sicherheit und weitere Partner versandt.

Workaround von Microsoft

Betroffen sei das SMBv3-Protokoll der folgenden Windows-Versionen: Windows 10 SAC (Semi-Annual Channel) 1903 und 1909 (32/64bit und ARM64) sowie Windows Server SAC 1903 und 1909. Windows 10 LTSC (Long Term Servicing Channel) 2016 und 2019 sowie Windows Server LTSC 2016 und 2019 sind von der Schwachstelle nicht betroffen.
SMB sei ein zentraler Bestandteil der Netzwerkdienste von Windows und komme unter anderem für den Zugriff auf Dateien auf Netzlaufwerken oder die Freigabe von Druckern zum Einsatz. SMB-Server/Client sei nicht mit Windows-Server/Client zu verwechseln. Auch unter Windows 10 komme die SMB-Server-Komponente zum Beispiel für die Freigabe von Netzlaufwerken zum Einsatz. Der von Microsoft bereitgestellte Workaround bewirkt, dass die Komprimierung von SMBv3 deaktiviert wird, informiert das BSI.
Seit Donnerstagabend (12. März 2020) stellt Microsoft laut BSI Sicherheitsupdates zur Behebung der Schwachstelle für alle betroffenen Windows-Versionen zur Verfügung. Aufgrund der Kritikalität der Schwachstelle empfiehlt das BSI, das Sicherheitsupdate umgehend und flächendeckend auf allen betroffenen Systemen einzuspielen.

(co)

Von Microsoft empfohlener Workaround
Sicherheitsupdates von Microsoft

Stichwörter: IT-Sicherheit, BSI, Microsoft, Schadprogramme, SMB-Clients, Windows