SMB-Backdoor

Mit dieser Benachrichtigung informieren wir Sie über Systeme in Ihrem Netzbereich, auf denen von Angreifern eine Hintertür (Backdoor) installiert wurde, über welche sie vollständigen Zugriff auf das betroffene System haben.

Am 14.03.2017 hat Microsoft ein Sicherheitsupdate für eine kritische Schwachstelle in Microsoft Windows veröffentlicht:

https://support.microsoft.com/de-de/help/4023262/how-to-verify-that-ms17-010-is-installed

Die Ausnutzung der Schwachstelle ermöglicht einem Angreifer, durch Senden speziell formulierter SMB-Anfragen an ein Windows-System beliebigen Programmcode auf diesem auszuführen, wenn Port 445/tcp offen aus dem Internet erreichbar ist.

Bei Systemen, auf welchen das oben genannte Sicherheitsupdate noch nicht eingespielt wurde, nutzen Angreifer die Schwachstelle aus, um eine Hintertür (Backdoor) zu installieren, über welche sie anschließend vollständigen Zugriff auf das System haben.

Über diesen Weg wurde z. B. auch die Ransomware "WannaCry" auf verwundbare Systeme geschleust.

Die Shadowserver Foundation [1] führt derzeit Scans nach Systemen im Internet durch, auf denen eine solche Hintertür installiert wurde. Als nationales CERT erhält CERT-Bund die Scan-Ergebnisse für Deutschland, um betroffene Systembetreiber benachrichtigen zu können.

Nachfolgend senden wir Ihnen eine Liste betroffener Systeme in Ihrem Netzbereich. Der Zeitstempel (Zeitzone UTC) gibt an, wann die Hintertür auf dem betroffenen System von Shadowserver identifiziert wurde.

Wir möchten Sie bitten, den Sachverhalt zu prüfen und Maßnahmen zur Bereinigung der Systeme zu ergreifen bzw. Ihre Kunden entsprechend zu informieren.

Betroffene Systeme sollten als vollständig kompromittiert angesehen und neu aufgesetzt werden. Alternativ kann ggf. eine Komplettsicherung (Backup) von einem Zeitpunkt vor der Kompromittierung zurückgespielt werden.

Links

[1] https://www.shadowserver.org/

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/smb-backdoor/