PsExec.exe und NET USE - Sicherheitsproblem mit Benutzerkennwort

Nummer:	**SEC-200212**	Status:	Freigegeben
Produktname:	**DBLAN - IT-Operator (DBL-IT-Operator.exe)**	Version:	1.2
Produktversion:	**1.6.200.210**		
Erstellt / Aktualisiert:	12.02.2020		

Erkennung /Problembeschreibung

Es scheint, dass es ein potenzielles Sicherheitsproblem in einer bestimmten Konfiguration von DBLAN - IT-Operator und Überwachungsrichtlinien in Verbindung mit dem Microsoft PsExec.exe-Tool und dem Net Use-Befehl gibt. Diese Konfiguration umfasst:

1. Gruppenrichtlinie: Computerkonfiguration \ Richtlinien \ Windows-Einstellungen \ Sicherheitseinstellungen \ Erweiterte Überwachungskonfiguration \ Detaillierte Überwachung \ Prozesserstellung überwachen
   - Folgende Überwachungsereignisse Konfigurieren: *(Aktiviert)*
     - Erfolg *(Aktiviert)*
     - Fehler *(Aktiviert)*

Die Kombination dieser Einstellungen ermöglicht es, Aktivitäten im Zusammenhang mit der Prozesserstellung und den zugehörigen Befehlen aufzuzeichnen und zu überwachen. Dies kann für Sicherheitsanalysen und die Erkennung von potenziell schädlichen Aktivitäten auf einem Windows-System nützlich sein.

2. Gruppenrichtlinie: Computerkonfiguration \ Richtlinien \ Administrative Vorlagen \ System \ Prozesserstellung überwachen \ Befehlszeile in Prozesserstellungsereignisse einschließen
   - Aktiviert

Es ist wichtig zu beachten, dass diese Einstellung ein leistungsstarkes Werkzeug für die Überwachung von Windows-Systemen ist, aber sie erzeugt auch eine erhebliche Menge an Protokolldaten. Daher ist es ratsam, die Protokollierung gezielt einzusetzen und sicherzustellen, dass die erzeugten Protokolle regelmäßig überprüft werden, um sicherheitsrelevante Ereignisse zu identifizieren und angemessen darauf zu reagieren.

3. DBLAN - IT-Operator \ Einstellungen \ Verwaltungskonto \ Verwaltungskonto (Local admin) \ Benutze Verwaltungskonto
   - Aktiviert

LogMonitor (Auszug aus dem Sysmon Log)
`C:\Program Files (x86) \PSTools\PsExec.exe -accepteula -nobanner -u sysdemo.org admin-xxx -p password \\WSTEST01 gpupdate /Target:Computer /Force`

Problem tritt auf, wenn folgende Optionen gestartet werden:

- Remote CMD und Ausführen (Remote Run)
- GP-Update und GP-Result
- Festplatte c: (Verbindung mit C$ vom Zielsystem)
- Nachricht an Benutzer
- Remote Skript und Remote Task
- SCCM - Agent => Action Schedule
- SMP - Agent => Basic Inventory und Aktualisierung der Konfiguration

Das Problem betrifft alle Installationen mit der Endzahl (Build) kleiner x.x.200.212

Lösung

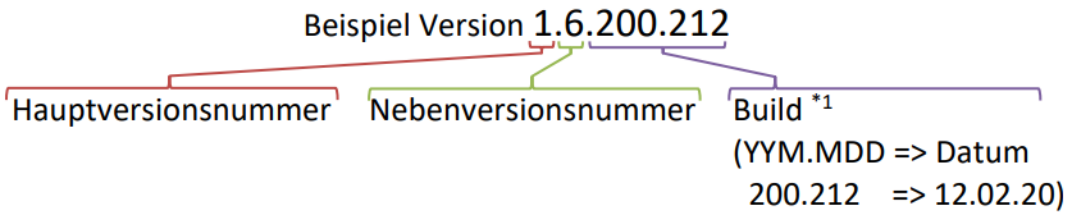
In der Version 1.6.200.212 und allen darauffolgenden Versionen wurde das Sicherheitsproblem erfolgreich behoben.

Wir empfehlen dringend, alle älteren Installationen des DBL-IT-Operators umgehend zu aktualisieren und das Kennwort des Verwaltungskontos zu ändern.

Information für die Teilnehmer des „DBLAN - IT-Operator Entwicklungsprogramms“:
Die Lösung ist bereits in die Versionen 1.7.xxx.xxx Beta und 2.0.xxx.xxx Alpha integriert worden. Bitte verwenden Sie Versionen mit der Endzahl (Build) x.x.200.212 oder höher.

Versionierung

Die Version setzt sich wie folgt zusammen:



*1 Build entspricht dem Publikationsdatum.

Kontakt

DBLAN
Damian Jan Brausch

Bahnhofstr. 33
D-79618 Rheinfelden (Baden)

Tel.: +49 7623 7416144
Fax: +49 7623 7416145

E-Mail: info@dblan.eu
Web: www.dblan.eu