

Backup und Archiv

Sicherheitsupdate am 5.10.2017



Backup und Archiv / Sicherheitsupdate am 5.10.2017

CVE-2016-8937 - Offline dictionary attack vulnerability

- Seit Oktober 2016 bei IBM intern bekannte Sicherheitslücke
- Am 02.10.2017 veröffentlicht IBM den Inhalt des CVE
 - „Offline dictionary attack vulnerability in IBM Spectrum Protect“
 - Kaum spezifizierte Angriffsvektoren
- Die Schwachstelle
 - Abgreifen von Passwort Hashes
 - „offline“ entschlüsseln der Hashes

Backup und Archiv / Sicherheitsupdate am 5.10.2017

Maßnahmen

- Lösungsvarianten ermitteln
 - „Zumachen“, selektives Freischalten, ...
- Entscheidungen durch Kompetenzträger herbeiführen
 - IT-Manager Security
 - IT-Manager Services
- Entscheidung umsetzen
 - Aktualisierung der Server zur Software-Fehler-Beseitigung
 - Erstellung neuer Dokumentation
 - Evaluierung von Softwareproblemen mit dem Hersteller (Server/Client)
- Risiken, Chancen und Aufwände
 - Neue Version, **neue Probleme**
 - Neue Version, neue Möglichkeiten *) effektiver Einsatz wird noch geprüft
 - Es gab keine andere Notwendigkeit für ein Update als die Sicherheitslücke
- Resumee
 - Aufgrund der neuen Probleme ... wünschen wir uns selbst die alte Version zurück

Backup und Archiv / Sicherheitsupdate am 5.10.2017

Aktuelle Hinweise zu IBM Spectrum Protect

- Unterstützte Client Versionen
 - 8.1.2 und höher
 - 7.1.8 und höher
- Neuer Authentisierungsalgorithmus
- SSL/TLS verschlüsselte Übertragung
 - Manueller Zertifikatsimport
- EOS TSM kleiner v7.1.8 insbesondere v6.4 und kleiner

**Vielen Dank
für Ihre Aufmerksamkeit**

