Newsletter des BSI

Nr. November 2011 /2, 29.11.2011 10:00 Uhr

Newsletter GSTOOL

SICHERHEITSWARNUNG
Sehr geehrte GSTOOL-Nutzer,

im Aufruf der Verschlüsselungsfunktion des GSTOOLs wurde eine Schwachstelle gefunden, die es Forschern der TU Darmstadt ermöglichte, mit dem GSTOOL verschlüsselte Dateien ohne Kenntnis des korrekten Schlüssels zu entschlüsseln.

Unter Ausnutzung der Schwachstelle ist ein Brute-Force-Angriff auf mit dem GSTOOL verschlüsselte Dateien erfolgversprechend möglich.

Davon betroffen sind alle Versionen des GSTOOL bis einschließlich Version 4.7. Es handelt sich bei der identifizierten Schwachstelle um einen Implementierungsfehler im GSTOOL

Der verwendete Verschlüsselungsalgorithmus selbst (Chiasmus) ist von diesem Angriff nicht betroffen und ist weiterhin sicher. Andere Produkte des BSI sind von der Schwachstelle nicht betroffen.

Die Verschlüsselungsfunktion im GSTOOL darf bis zum Erscheinen eines Patches nicht mehr verwendet werden.

Der Patch wird derzeit erstellt. Nach genauer Prüfung soll er in das Servicepack 3 integriert werden.

Empfehlung:
1) Eventuell öffentlich zugängliche, mit dem GSTOOL verschlüsselte, Dateien sollten zurückgezogen werden.
2) Die Verschlüsselung von GSTOOL Dateien sollte bis zum Erscheinen eines Patches durch eine externe Verschlüsselungssoftware (z.B. Chiasmus) erfolgen.
3) In Kürze wird ein Servicepack für das GSTOOL erscheinen, das die Schwachstelle behebt und umgehend eingespielt werden sollte.

Mit freundlichen Grüßen

Ihr GSTOOL-Team