Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

BSI IT-Sicherheitswarnung 27/2011

Schwachstelle im GSTOOL

25.11.2011
Version: 1.0

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Lagezentrum
Godesberger Allee 185-189, 53175 Bonn

Telefon: +49 (0)228 99 9582 5110
Telefax: +49 (0)228 99 9582 7025
E-Mail: lagezentrum@bsi.bund.de
Internet: https://www.bsi.bund.de
https://www.cert-bund.de

Datum:	25.11.11	Berichterstatter:	BSI-Lagezentrum

Schwachstelle im GSTOOL*		
IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs. Maßnahmen wurden durch das BSI in die Wege geleitet.	Die vorliegende Sicherheitswarnung enthält Informationen zu einer Schwachstelle im GSTOOL.	2

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau. Es erfolgen ständig Angriffsversuche und erfolgreiche Angriffe. Schwachstellen werden bekannt, kleinere Sicherheitsvorfälle treten auf, aber Besonderheiten fehlen.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs. Maßnahmen wurden durch das BSI in die Wege geleitet.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs. Dezentrale Maßnahmen sind zu ergreifen (i.d.R. Warnmeldung / Sonderbericht zur zeitkritischen Reaktion).
4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden (nur für Warnmeldung / Sonderbericht zur zeitkritischen Reaktion).

Sachverhalt

Im Aufruf der Verschlüsselungsfunktion im GSTOOL[1] wurde ein Fehler gefunden, der 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 möglich. Davon betroffen sind alle Versionen des GSTOOL bis einschließlich V 4.5.

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.

Bewertung

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

Empfehlung

Das BSI-Lagezentrum empfiehlt, die folgenden Empfehlungen umzusetzen:

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[2]) erfolgen.

3) In Kürze wird ein Servicepack für das GSTOOL erscheinen, das die Schwachstelle behebt und umgehend eingespielt werden sollte.

URLs:

[1] https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/gstool_node.html
[2] https://www.bsi.bund.de/ContentBSI/Themen/ProdukteTools/Chiasmus/Chiasmus.html

Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

BSI IT-Sicherheitswarnung 27/2011

Schwachstelle im GSTOOL

29.11.2011
Version: 1.1

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Lagezentrum
Godesberger Allee 185-189, 53175 Bonn

Telefon: +49 (0)228 99 9582 5110
Telefax: +49 (0)228 99 9582 7025
E-Mail: lagezentrum@bsi.bund.de
Internet: https://www.bsi.bund.de
https://www.cert-bund.de

Datum:	29.11.11	Berichterstatter:	BSI-Lagezentrum

Schwachstelle im GSTOOL*		
IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs. Maßnahmen wurden durch das BSI in die Wege geleitet.	Die vorliegende Sicherheitswarnung enthält Informationen zu einer Schwachstelle im GSTOOL.	2

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau. Es erfolgen ständig Angriffsversuche und erfolgreiche Angriffe. Schwachstellen werden bekannt, kleinere Sicherheitsvorfälle treten auf, aber Besonderheiten fehlen.
2 / Gelb: IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs. Maßnahmen wurden durch das BSI in die Wege geleitet.
3 / Orange: Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs. Dezentrale Maßnahmen sind zu ergreifen (i.d.R. Warnmeldung / Sonderbericht zur zeitkritischen Reaktion).
4 / Rot: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden (nur für Warnmeldung / Sonderbericht zur zeitkritischen Reaktion).

Sachverhalt

Im Aufruf der Verschlüsselungsfunktion im GSTOOL[1] wurde ein Fehler gefunden, der 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 in sehr kurzer Zeit möglich.

UPDATE vom 29.11. Version 1.1:

Von der Schwachstelle betroffen sind alle GSTOOL- Versionen bis einschließlich V 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.

Bewertung

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

Empfehlung

Das BSI-Lagezentrum empfiehlt, die folgenden Empfehlungen umzusetzen:

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[2]) erfolgen.

3) In Kürze wird ein Servicepack für das GSTOOL erscheinen, das die Schwachstelle behebt und umgehend eingespielt werden sollte.

URLs:

[1] https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/gstool_node.html
[2] https://www.bsi.bund.de/ContentBSI/Themen/ProdukteTools/Chiasmus/Chiasmus.html