

Presseinformation:

DoS-Attacken: Komprimierte Bomben legen Rechner lahm

Hohenbrunn b. München, 03.02.2004

Die AERAssec Network Services and Security GmbH aus Hohenbrunn b. München hat jetzt weitere Untersuchungen zum Thema „Dekomprimierungsbomben“ durchgeführt – mit teilweise beunruhigenden Ergebnissen.

Dr. Matthias Leu, Geschäftsführer der AERAssec, warnt: „Gegenüber solchen Bomben ist nicht nur Anti-Virus Software anfällig, sondern auch andere Software wie z.B. Browser ist auf sehr stark komprimierte Daten teilweise nicht vorbereitet. Dieses gilt für unterschiedlichste Komprimierungsverfahren und liegt daran, dass auch heutige Software Anomalien beim Dekomprimieren nicht immer erkennt“.

Bekannt ist, dass einige Anti-Virus Programme bei der Untersuchung von Dateien im bzip2-Format keine Größenbegrenzung für das Entpacken der Daten implementiert haben. Dadurch besteht für Angreifer die Möglichkeit, den Anti-Virus Server durch solche Bomben auszuschalten. Speziell Unternehmen mit einem zentralen Internetzugang und der Untersuchung übertragener E-Mails auf Schadcode, wären über E-Mail nicht mehr erreichbar. Die jetzt von AERAssec veröffentlichten Ergebnisse zeigen, dass durch anders konstruierte Bomben weitere Klassen von Applikationen betroffen sind.

Nicht alle Software-Hersteller berücksichtigen in ihren Produkten, dass eine Datei von 5.828 Byte entpackt 100 Gigabyte ergeben kann. Dr. Matthias Leu dazu: „Es ist an der Zeit, dass die Hersteller mit solchen Gemeinheiten rechnen. Es ist eigentlich nur eine Frage der Zeit, dass auch die Programmierer von Schadcode auf diese Idee kommen“. Insofern geht von AERAssec ein Appell speziell an die Software-Hersteller, hier möglichst umgehend ihre Produkte zu testen und die ggf. notwendigen Verbesserungen zu implementieren.

Über AERAssec:

Die AERAssec GmbH, gegründet 2000, hat ihren Sitz in Hohenbrunn bei München. Die hier arbeitenden Ingenieure und IT-Spezialisten richten Sicherheitslösungen vor Ort auf verschiedenen Plattformen ein. Entsprechender Support, sowie umfassende Beratungs- und Schulungsangebote ergänzen das Portfolio.

Weitere Informationen zu AERAssec finden Sie unter www.aerasesc.de.

Das Advisory steht im Internet unter <http://www.aerasesc.de/security/?id=ae-200402-006> zum Download bereit.

Der Text enthält 1.966 Zeichen (2.245 Zeichen mit Leerzeichen).

Abdruck honorarfrei. Über ein Belegexemplar würden wir uns freuen!

Kontakt:

AERAssec Network Services and Security GmbH

Dr. Matthias Leu

Wagenberger Strasse 1, D-85662 Hohenbrunn

Telefon: (08102) 895 190, Telefax: (08102) 895199

E-Mail: info@erasesc.de