

DARC-Alert Slowloris 7. Juli 2009

Einführung

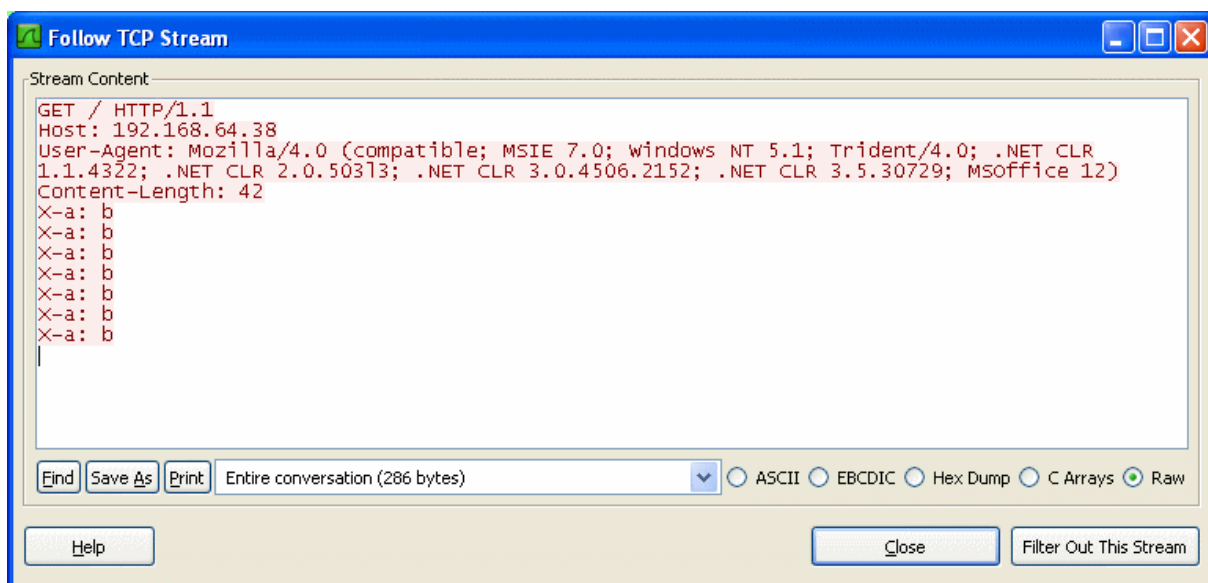
Am 17. Juni wurde das Tool Slowloris veröffentlicht, mit dem Denial-of-Service-Angriffe gegen Webserver gefahren werden können.

Das DARC (DenyAll Research Center) hat eine technische Analyse des Tools und der Angriffsmethode durchgeführt.

Beschreibung des Angriffs

Slowloris ist ein Perl-Skript, das auf jeder *nix-Plattform ausgeführt werden kann.

Der Angriff erfolgt durch Einleitung von HTTP-Requests, die nicht abgeschlossen werden. Die permanente Übertragung von HTTP-Headern hat zur Folge, dass die Verbindungen offen bleiben. Die nachstehende Abbildung zeigt den Ablauf eines solchen Requests, wobei der „X-a: b“-Header deutlich zu erkennen ist, den das Tool verwendet.



```
Stream Content
GET / HTTP/1.1
Host: 192.168.64.38
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; Trident/4.0; .NET CLR
1.1.4322; .NET CLR 2.0.50313; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MSoffice 12)
Content-Length: 42
X-a: b
X-a: b
X-a: b
X-a: b
X-a: b
X-a: b
X-a: b
X-a: b
X-a: b
```

Der Apache-Webserver reicht Anfragen erst dann an die bearbeitenden Module weiter, wenn sie vollständig sind. Er ist also anfällig für diesen Angriff, da er aktive Verbindungen, die von dem Tool hergestellt wurden, nicht freigibt. Aus demselben Grund können auch keine Apache-Sicherheitsmodule eingesetzt werden.

Sobald der Angriff gestartet wurde, hält der Zielsever die hergestellten Verbindungen im Status ESTABLISHED geöffnet.

Bereits nach kurzer Zeit ist der Server nicht mehr erreichbar. Dieser Zustand bleibt für die Dauer des Angriffs bestehen.

Gegenmaßnahmen

Am Samstag, 20. Juni, stellte das DARC für DenyAll-Kunden einen Workaround bereit. Dieser Workaround, der auf Paketfilterung und Mechanismen zur Verbindungsbegrenzung basiert, ermöglichte es, Websites vor dem Angriff zu schützen.

Am 26. Juni wurde für sämtliche Produkte von DenyAll ein Patch verfügbar gemacht. Nach einer einwöchigen Testphase wurde dieser Patch heute veröffentlicht.

Somit können nun alle Kunden von DenyAll vor diesem Angriff geschützt werden, ebenso wie vor jeglichen Varianten, die auf der gleichen Technik beruhen.

Dies ist der erste Patch für Apache-basierte Produkte, der gegen diesen Angriff veröffentlicht wurde.

Fazit

Bislang ist keine offizielle, Apache-native Lösung für dieses Problem verfügbar, da dazu umfangreiche Änderungen in der internen Struktur des Webserver erforderlich sind.

Dank der von seinem Research Center durchgeführten Analyse ist DenyAll der einzige Hersteller, der eine Lösung zur Abwehr solcher Angriffe für alle seine produktiven Plattformen veröffentlicht hat.

Über das DARC

Das DenyAll Research Center ist eine hausinterne Abteilung von DenyAll, die sich speziell der Analyse von Bedrohungen sowie entsprechenden Abwehrmaßnahmen widmet.

Die nunmehr zehnjährige Forschungstätigkeit dieser Abteilung hat Deny All in die Lage versetzt, Security-Engines für Webanwendungen zu entwickeln, die dem Spitzenstand der Technik entsprechen.

Über Deny All:

Deny All ist der europäische Marktführer für Web, XML und FTP Application Firewalls. Das Unternehmen liefert bewährte Lösungen, die weltweit und in allen Branchen von großen Unternehmen und Organisationen eingesetzt werden. Die Produkte von Deny All, als Software und Appliances erhältlich, gewährleisten den Schutz, die Authentifizierung und die Beschleunigung von Transaktionen im Internet, Extranet und Intranet

Die leicht installierbaren Lösungen von Deny All garantieren maximalen Schutz vor bekannten und unbekanntem Angriffen, die über die HTTP(S)-, SOAP/XML- und FTP(S)-Datenströme erfolgen. Mittlerweile schützen rWeb-Implementierungen mehr als 10.000 Web-Anwendungen weltweit.

Der Hauptsitz von Deny All befindet sich in Paris. Darüber hinaus unterhält das Unternehmen europäische Niederlassungen in Deutschland, den nordischen Ländern, Spanien sowie den Benelux-Ländern und verfügt über aktive Partnerschaften in ganz Europa.

Das Unternehmen ist Mitglied der CLUSIF, OSSIR und OWASP, der SAP Global Security Alliance und der Liberty Alliance.

Pressekontakt:

Ursula Kafka/Janina Rogge

Kafka Kommunikation GmbH & Co KG

+49 89 7675 9434

mailto: ukafka@kafka-kommunikation.de

jrogge@kafka-kommunikation.de