Deny All releases a patch against Slowloris, an attack against Web servers

Press Flash,

Paris, 3th of July 2009

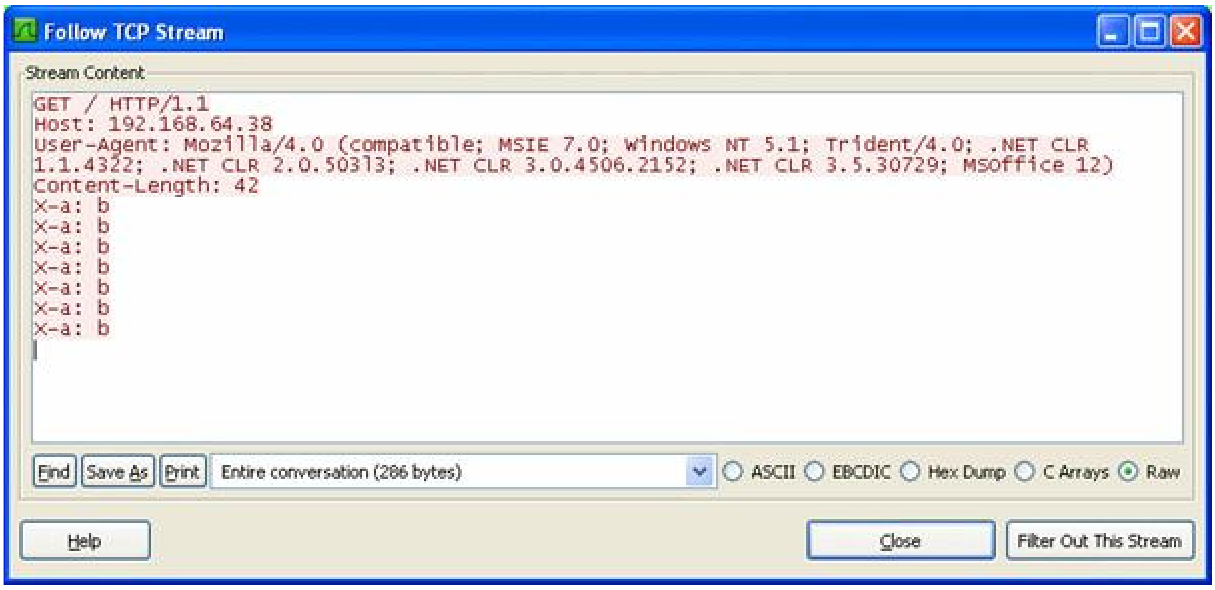
The slowloris tool, which implements a denial of service attack against Web servers, was published on June the 17th.

The DARC (Deny All Research Center), division of Deny All which focuses on threat analysis and mitigation, performed a technical analysis of the tool and the concept of the attack. After 10 years of activity, researches performed by this department have lead to the design of state-of-the art Web application security engines.

Attack description

Slowloris is a perl script which can be run on any *nix platform.

The attack consists in initiating HTTP requests without closing them. The connection is then left opened thanks to recurring transmission of HTTP headers. The figure below shows the trace of the request and clearly identifies the "X-a: b" header used by the tool.



```
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
```

Entire conversation (286 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

The Apache Web server sends requests to processing modules only once they are completed. As a consequence it is vulnerable to the attack as it doesn't free active connections established by the attack tool. Apache security modules cannot be applied for the same reasons.

Once the attack is launched the target server holds open connections in state ESTABLISHED.

After a short amount of time the server becomes unreachable. This status lasts for the duration of the attack.

Mitigation

On Saturday, June 20th, the DARC provided Deny All customers with a workaround. This workaround, based on packet filtering and connection limit mechanisms, made it possible to prevent web sites from being impacted by this attack.

On June 26th, a patch was made available for all Deny All products. This patch has been publicly released today after one week of testing.

Therefore all Deny All customers can now be protected from this attack and any variant based on the same technique.

This is the first release of a patch for an Apache-based products against this attack.

As of today no official Apache native solution is available, as it requires heavy internal changes.

Thanks to the analysis performed by its research center, Deny All is the only editor which has released such solution for all its production platforms.

About Deny All

Pioneer of WAF (Web Application Firewall), Deny All is now the European leader in the protection and accelerating Web applications, XML and FTP. Deny All provides solutions to large accounts globally, on all sectors. Its products, available as software or appliance, ensure protection, authentication and transaction acceleration on Internet, extranet and intranet. The Deny All solutions are easy to install and guarantee the highest level of protection against known and unknown attacks through a filter of HTTP(S), SOAP / XML and FTP(S). Today, Deny All solutions protect more than 10 000 web applications around the world.

With headquarters in Paris, Deny All is present in most European countries through local teams in Germany, Benelux, Spain and Nordic countries and through its network of partners.

Deny All is a member of CLUSIF, the OWASP, the OSSIR, the SAP Global Security Alliance and Liberty Alliance.

Contacts presse :	
OXYGEN	**DENY ALL**
Audrey Sliwinski / Tatiana Graffeuil Tél. : +33 (0)1 41 11 37 84 / 37 89 audrey@oxygen-rp.com tgraffeuil@oxygen-rp.com **www.oxygen-rp.fr**	Delphine Hosatte Tél. : +33 (0)1 40 07 49 90 dhosatte@denyall.com **www.denyall.com**