Security Research Advisory – September 1st, 2011

Apache Denial of Service

What happened?

A vulnerability leading to a Denial of Service (DOS) was recently discovered. The DOS is very efficient, because very few resources are required on the attacker's end to interrupt the service of a high capacity server. Tools exploiting this vulnerability are already available. A patch will be released in the coming days for Apache versions 2.0 and 2.2. No patch is planned at this point in time however for version 1.3.

Attack description

The attack leverages an error in the management of the "range" header. An attack can be performed whenever the content of the answer is buffered, namely when using mod_deflate, i.e. when compressing server responses.

Mitigation

This attack is blocked by default by rWeb (3.x and 4.0) and sProxy (2.6 and 4.0). The DARC team simply recommends that customers verify that the rule limiting the maximal length of headers was not deactivated by mistake. The restrictions imposed by this filter will block attacks using a large number of "range" instructions. In that context, the attack cannot be efficient and the additional memory usage will remain limited (1% to 2% maximum).

About the DARC

The Deny All Research Center (DARC) is an internal division of Deny All, which focuses on threat analysis and mitigation. Over the last 10 years, this department's research has contributed to the design of state-of-the art Web application security solutions. More information on Deny All can be found at www.denyall.com