The Lock May be Broken

Or Katz, 2012-12-02

A couple of weeks ago, a new security advisory was published: CVE-2012-0053 - “Apache HttpOnly Cookie Disclosure”. While the severity of this vulnerability is just “medium”, there are some things that we can learn from it.

As far as I see it, this vulnerability actually uses a more sophisticated approach in order to steal sensitive information. It suggests an exploit proof of concept that combines two attack methods:

> 1. A well-known application security vulnerability named “Cross-Site Scripting (XSS)”.

> 2. A newly introduced vulnerability in Apache, where sending a cookie HTTP-Header that is too long, the HttpOnly cookie value, is returned by the web server in a “400 Bad Request” response page.

From the OWASP page on HttpOnly - Mitigating the Most Common XSS attack using HttpOnly

“The majority of XSS attacks target theft of session cookies. A server could help mitigate this issue by setting the HTTPOnly flag on a cookie it creates, indicating the cookie should not be accessible on the client.

If a browser that supports HttpOnly detects a cookie containing the HttpOnly flag, and client side script code attempts to read the cookie, the browser returns an empty string as the result. This causes the attack to fail by preventing the malicious (usually XSS) code from sending the data to an attacker's website.”

So the HttpOnly cookie that is not supposed to be accessed by Java-Script on client browser can be accessed when exploiting this vulnerability. In other words, the lock may be broken, and the mechanism that is supposed to prevent an attack, in some circumstances, can be bypassed. This leads me to say that while security countermeasures are becoming more and more sophisticated over the years, security vulnerabilities and their exploits are becoming more and more elusive.

Web Application Firewalls were designed from the beginning to solve such zero-day vulnerabilities presenting multi layered protection for the web application by combining signature based, HTTP protocol constraints and web application behavioral anomalies protection.

From BIG-IP Application Security Manager perspective, this vulnerability can be easily mitigated by performing the following:

> i. Using Cross-Site Scripting signatures in order to mitigate Cross-Site Scripting vulnerabilities.

ii. Applying a security policy that limits the header's length.

iii. Creating a custom error page when this violation occurs.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com