Security Sidebar: Hands Up...This is a HEIST

John Wagnon, 2016-08-08

The Fear…

The newly discovered HEIST (**H**TTP **E**ncrypted **I**nformation can be **S**tolen through **T**CP-Windows) vulnerability is making some noise, and people are rightfully freaked out a little bit. HEIST is accomplished purely in the browser and attacks SSL/TLS channels to expose sensitive encrypted data such as emails, Social Security Numbers, etc. It works by hiding a JavaScript file on a webpage (made to look safe in an advertisement or maybe even hosted directly on a site), and enticing the user to interact with said JavaScript file. Once the interaction has happened, the malicious code queries a variety of web pages and measures the exact size of the encrypted data that those pages transmit. Once the size of the responses is known, the attackers can use a previously-identified compression exploit (such as CRIME or BREACH) to gain access to the data inside those encrypted packets.

Probably the most interesting characteristic of this vulnerability is that it removes the need for a "man-in-the-middle" position. Until now, this compression-based exploit required the attacker to be able to actively manipulate the traffic passing between the Web server and end user. One of the researchers who discovered this exploit said it like this: "Before, the attacker needed to be in a Man-in-the-Middle position to perform attacks such as CRIME and BREACH. Now, by simply visiting a website owned by a malicious party, you are placing your online security at risk."

The most damaging aspect of HEIST is found by exploiting BREACH, as it allows the attacker to read out CSRF tokens. Depending on the functionality offered by the website, knowing the CSRF token could allow the attacker to take over the complete account of the victim.

The simple solution to all this is to tell users to never visit a website owned by a malicious party, right? Yeah, right. So, what can you do to mitigate this vulnerability?

The Redemption…

Fortunately, the BIG-IP offers several countermeasures to help protect from this HEIST vulnerability. Because HEIST relies on compression attacks like CRIME and BREACH, the first countermeasure is to disable HTTP compression on user input pages. Static content can still be compressed, though.

Next, configure your BIG-IP ASM for CSRF protection. One of the ways BIG-IP ASM mitigates CSRF attacks is by adding a random CSRF token to every URL. For example, if an HTML response page contains the following URI reference:

```
a href="https://host.domain.com/default.aspx"
```

The BIG-IP ASM (with CSRF protection enabled) will rewrite the URI reference to appear similar to the following:

```
a href="https://host.domain.com/default.aspx?CSRT=17017154763700437104"
```

This token cannot be guessed in advance by an attacker and therefore makes the CSRF attack almost impossible.

The BIG-IP ASM also has a domain cookie protection feature. If an attacker were to use HEIST (or some other exploit) to get the authentication cookie, he must also obtain the rotating ASM cookie that contains a signature of all the other cookies.

It’s a scary world out there, but it’s a little less scary when the BIG-IP is protecting your critical web applications!

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

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113