Suricata - Bug #308

gzipped http content does not get unzipped and processed

08/02/2011 03:07 AM - Sander Klein

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category:
Target version: 1.2beta1
Affected Versions:
Effort:
Difficulty:
Label:

Description
Suricata does not unzip and process gzipped http content. I tried versions: 1.0.4, 1.0.5, 1.1bet2, 1.1 git clone on 20110801.

For testing I used this rule:

alert tcp any any -> any any (msg:"TEST SUCCESFULL - inspecting body";flow:stateless; content:"implementation"; nocase;)

I requested my own web page using:

curl http://www.roedie.nl <- Triggers the alert

curl --compressed http://www.roedie.nl <- Does not trigger the alert.

I've attached a pcap with the compressed request.

History

#1 - 08/04/2011 12:55 PM - Anoop Saldanha

This won't match. The content keyword is matched against the raw stream/payload, while the data is gzipped response body. So the right way to do this would be to have a keyword like "http_server_body" just like how we have "http_client_body" currently, and use it this way

alert tcp any any -> any any (content:implementation; http_server_body;)

which would now search the gunzip'ed server response body for the string "implementation"

We don't support such a keyword as yet. You can probably raise a feature request.

#2 - 08/04/2011 02:55 PM - Sander Klein

I think I misunderstood http://www.openinfosecfoundation.org/index.php/component/content/article/1-latest-news/82-suricata-beta-available then.

The page says 'Gzip Decompression - The HTP Parser will decode Gzip compressed streams, allowing much more detailed matching within the engine.' I thought it meant Suricata would unzip http requests which are zipped by mod_deflate. If I'm wrong then indeed it's not a bug and I should raise a feature request.

#3 - 08/05/2011 12:39 AM - Anoop Saldanha

Sander Klein wrote:

I think I misunderstood http://www.openinfosecfoundation.org/index.php/component/content/article/1-latest-news/82-suricata-beta-available then.

The page says 'Gzip Decompression - The HTP Parser will decode Gzip compressed streams, allowing much more detailed matching within the engine.' I thought it meant Suricata would unzip http requests which are zipped by mod_deflate.

Your understanding is right here. Suricata does decompress the gzipped response(to be more precise, Suricata's http engine, libhtp, does the decompression), but it doesn't use this decompressed response to match against any keywords, since it currently has no keywords that inspects the response body.

If I'm wrong then indeed it's not a bug and I should raise a feature request.

Yes, it's not a bug, but a feature request for a new "keyword"(http_server_body probably), that would allow suricata to inspect the response body. Once we have such a keyword you can use it as "content:implementation; http_server_body;", following which this keyword would then inspect the deflated response for "implementation".
http_server_body and file_data have been implemented. Both inspect the normalized/dechunked/unzipped response body.

Files

<table>
<thead>
<tr>
<th>File Name</th>
<th>Size</th>
<th>Date</th>
<th>Author</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.roedie.nl-20110802.pcap">www.roedie.nl-20110802.pcap</a></td>
<td>10.4 KB</td>
<td>08/02/2011</td>
<td>Sander Klein</td>
</tr>
</tbody>
</table>