test

test

test
Golden Egg Labs, INC.

https://goldenegglabs.com

August 08, 2023

Contents

1 Document Overview **3**

2 Executive Summary **4**

2.1 Summary of Findings Identified 6

2.2 Scope 6

2.2.1 In Scope 6

2.2.2 Out of Scope 6

2.3 Methodology 7

2.4 Recommendations 8

3 Findings and Risk Analysis **9**

4 Additional Notes **10**

1 Document Overview

TBC

2 Executive Summary

<table id="response" class="table caption-top table-striped table-hover" style="width:100%"> <caption>Embedded GoAhead HTTP Host Header Injection</caption> <thead> <tr> <th>index</th> <th>Hostname</th> <th>IP address</th> <th>Type</th> <th>Target Hostname</th> </tr> </thead> <tbody> <tr> <th>0</th> <td>grafana.streammyflr.org</td> <td>188.114.97.13</td> <td>A</td> <td>grafana.streammyflr.org</td> </tr> <tr> <th>1</th> <td>streammyflr.org</td> <td>2606:4700:50::adf5:3a38</td> <td>NS</td> <td>adi.ns.cloudflare.com</td> </tr> <tr> <th>2</th> <td>portainer.streammyflr.org</td> <td>172.67.222.127</td> <td>A</td> <td>portainer.streammyflr.org</td> </tr> <tr> <th>3</th> <td>netdata.streammyflr.org</td> <td>2606:4700:3030::ac43:de7f</td> <td>AAAA</td> <td>netdata.streammyflr.org</td> </tr> <tr> <th>4</th> <td>grafana.streammyflr.org</td> <td>2a06:98c1:3120::5</td> <td>AAAA</td> <td>grafana.streammyflr.org</td> </tr> <tr> <th>5</th> <td>streammyflr.org</td> <td>172.67.222.127</td> <td>A</td> <td>streammyflr.org</td> </tr> <tr> <th>6</th> <td>streammyflr.org</td> <td>104.21.70.100</td> <td>A</td> <td>streammyflr.org</td> </tr> <tr> <th>7</th> <td>streammyflr.org</td> <td>2a06:98c1:50::ac40:2038</td> <td>NS</td> <td>adi.ns.cloudflare.com</td> </tr> <tr> <th>8</th> <td>streammyflr.org</td> <td>2803:f800:50::6ca2:c038</td> <td>NS</td> <td>adi.ns.cloudflare.com</td> </tr> <tr> <th>9</th> <td>royalty.streammyflr.org</td> <td>172.67.222.127</td> <td>A</td> <td>royalty.streammyflr.org</td> </tr> <tr> <th>10</th> <td>grafana.streammyflr.org</td> <td>2606:4700:3033::6815:4664</td> <td>AAAA</td> <td>grafana.streammyflr.org</t </tr> <tr> <th>11</th> <td>netdata.streammyflr.org</td> <td>188.114.97.1</td> <td>A</td> <td>netdata.streammyflr.org</td> </tr> <tr> <th>12</th> <td>royalty.streammyflr.org</td> <td>2606:4700:3033::6815:4664</td> <td>AAAA</td> <td>royalty.streammyflr.org</td> </tr> <tr> <th>13</th> <td>royalty.streammyflr.org</td> <td>2606:4700:3030::ac43:de7f</td> <td>AAAA</td> <td>royalty.streammyflr.org</td> </tr> <tr> <th>14</th> <td>snipe.streammyflr.org</td> <td>2606:4700:3030::ac43:de7f</td> <td>AAAA</td> <td>snipe.streammyflr.org</td> </tr> <tr> <th>15</th> <td>grafana.streammyflr.org</td> <td>188.114.96.13</td> <td>A</td> <td>grafana.streammyflr.org</td> </tr> <tr> <th>16</th> <td>grafana.streammyflr.org</td> <td>172.67.222.127</td> <td>A</td> <td>grafana.streammyflr.org</td> </tr> <tr> <th>17</th> <td>streammyflr.org</td> <td>2803:f800:50::6ca2:c1da</td> <td>NS</td> <td>oswald.ns.cloudflare.com</td> </tr> <tr> <th>18</th> <td>streammyflr.org</td> <td>2606:4700:58::adf5:3bda</td> <td>NS</td> <td>oswald.ns.cloudflare.com</td> </tr> <tr> <th>19</th> <td>streammyflr.org</td> <td>173.245.58.56</td> <td>NS</td> <td>adi.ns.cloudflare.com</td> </tr> <tr> <th>20</th> <td>hls.streammyflr.org</td> <td>45.63.58.149</td> <td>A</td> <td>hls.streammyflr.org</td> </tr> <tr> <th>21</th> <td>snipe.streammyflr.org</td> <td>104.21.70.100</td> <td>A</td> <td>snipe.streammyflr.org</td> </tr> <tr> <th>22</th> <td>icecast.streammyflr.org</td> <td>91.121.35.81</td> <td>A</td> <td>icecast.streammyflr.org</td> </tr> <tr> <th>23</th> <td>grafana.streammyflr.org</td> <td>2606:4700:3030::ac43:de7f</td> <td>AAAA</td> <td>grafana.streammyflr.org</t </tr> <tr> <th>24</th> <td>www.streammyflr.org</td> <td>2a06:98c1:3121::7</td> <td>AAAA</td> <td>www.streammyflr.org</td> </tr> <tr> <th>25</th> <td>streammyflr.org</td> <td>2803:f800:50::6ca2:c038</td>

<td>SOA</td> <td>adi.ns.cloudflare.com</td> </tr> <tr> <th>26</th> <td>phpmyadmin.streammyflr.org</td>
<td>104.21.70.100</td> <td>A</td> <td>phpmyadmin.streammyflr.org</td> </tr> <tr> <th>27</th>
<td>netdata.streammyflr.org</td> <td>104.21.70.100</td> <td>A</td> <td>netdata.streammyflr.org</td>
</tr> <tr> <th>28</th> <td>streammyflr.org</td> <td>2606:4700:3033::6815:4664</td> <td>AAAA</td>
<td>streammyflr.org</td> </tr> <tr> <th>29</th> <td>www.streammyflr.org</td> <td>2606:4700:3033::6815:4664</td>
<td>AAAA</td> <td>www.streammyflr.org</td> </tr> <tr> <th>30</th> <td>snipe.streammyflr.org</td>
<td>172.67.222.127</td> <td>A</td> <td>snipe.streammyflr.org</td> </tr> <tr> <th>31</th>
<td>snipe.streammyflr.org</td> <td>2606:4700:3033::6815:4664</td> <td>AAAA</td> <td>snipe.streammyflr.org</td>
</tr> <tr> <th>32</th> <td>streammyflr.org</td> <td>2a06:98c1:50::ac40:2038</td> <td>SOA</td>
<td>adi.ns.cloudflare.com</td> </tr> <tr> <th>33</th> <td>netdata.streammyflr.org</td>
<td>2606:4700:3033::6815:4664</td> <td>AAAA</td> <td>netdata.streammyflr.org</td> </tr>
<tr> <th>34</th> <td>snipe.streammyflr.org</td> <td>2a06:98c1:3121::9</td> <td>AAAA</td>
<td>snipe.streammyflr.org</td> </tr> <tr> <th>35</th> <td>streammyflr.org</td> <td>2606:4700:3030::ac43:de7f</td>
<td>AAAA</td> <td>streammyflr.org</td> </tr> <tr> <th>36</th> <td>grafana.streammyflr.org</td>
<td>2a06:98c1:3121::5</td> <td>AAAA</td> <td>grafana.streammyflr.org</td> </tr> <tr> <th>37</th>
<td>portainer.streammyflr.org</td> <td>104.21.70.100</td> <td>A</td> <td>portainer.streammyflr.org</td>
</tr> <tr> <th>38</th> <td>streammyflr.org</td> <td>173.245.58.56</td> <td>SOA</td> <td>adi.ns.cloudflare.com</td>
</tr> <tr> <th>39</th> <td>netdata.streammyflr.org</td> <td>188.114.96.0</td> <td>A</td>
<td>netdata.streammyflr.org</td> </tr> <tr> <th>40</th> <td>www.streammyflr.org</td>
<td>2606:4700:3030::ac43:de7f</td> <td>AAAA</td> <td>www.streammyflr.org</td> </tr> <tr>
<th>41</th> <td>streammyflr.org</td> <td>172.64.32.56</td> <td>NS</td> <td>adi.ns.cloudflare.com</td>
</tr> <tr> <th>42</th> <td>streammyflr.org</td> <td>2a06:98c1:50::ac40:21da</td> <td>NS</td>
<td>oswald.ns.cloudflare.com</td> </tr> <tr> <th>43</th> <td>phpmyadmin.streammyflr.org</td>
<td>2606:4700:3030::ac43:de7f</td> <td>AAAA</td> <td>phpmyadmin.streammyflr.org</td>
</tr> <tr> <th>44</th> <td>www.streammyflr.org</td> <td>172.67.222.127</td> <td>A</td>
<td>www.streammyflr.org</td> </tr> <tr> <th>45</th> <td>streammyflr.org</td> <td>108.162.192.56</td>
<td>SOA</td> <td>adi.ns.cloudflare.com</td> </tr> <tr> <th>46</th> <td>portainer.streammyflr.org</td>
<td>2606:4700:3030::ac43:de7f</td> <td>AAAA</td> <td>portainer.streammyflr.org</td> </tr>
<tr> <th>47</th> <td>phpmyadmin.streammyflr.org</td> <td>172.67.222.127</td> <td>A</td>
<td>phpmyadmin.streammyflr.org</td> </tr> <tr> <th>48</th> <td>www.streammyflr.org</td>
<td>2a06:98c1:3120::7</td> <td>AAAA</td> <td>www.streammyflr.org</td> </tr> <tr> <th>49</th>
<td>netdata.streammyflr.org</td> <td>172.67.222.127</td> <td>A</td> <td>netdata.streammyflr.org</td>
</tr> </tbody> </table>

2.1 Summary of Findings Identified

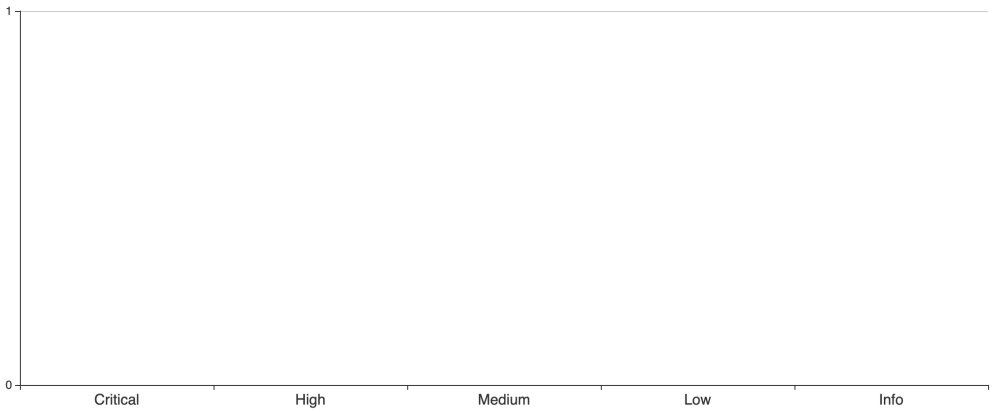

Figure 1: Executive Summary

Figure 2: Breakdown by Categories

2.2 Scope

2.2.1 In Scope

TBC

2.2.2 Out of Scope

TBC

2.3 Methodology

TBC

2.4 Recommendations

TBC

3 Findings and Risk Analysis

4 Additional Notes