PDF Export for report 1438600

Edge Server non-HTTPS requests to origin server being MITMed by a ISP (AIRTEL India)

State	N/A
Reported by	Anunay (anunayj)
Reported to	CloudflareTest (cloudflaretest)
Submitted at	(ISO-8601)
Asset	
References	
Weakness	Man-in-the-Middle
Severity	low
CVE IDs	

Requests to the following domains (non-exhaustive) served by Cloudflare gave me an unexpected reply:

1. https://usebottles.com
2. https://www.worldql.com

The website has been blocked as per order of Ministry of Electronics and Information Technology under IT Act, 2000.

This would be normal under HTTP since my ISP likes blocking domains, but these requests were made over HTTPS (and appeared to have a valid Cloudflare certificate) and actually hit Cloudflare Anycast Addresses (172.67.190.57, 104.21.19.214). I tried these same requests with another ISP and didn't run into these issues.

However I am concerned what this means is, an edge server which I presume is inside my ISPs network is MITMing requests between the origin server <-> edge server which might happen over HTTP if the domain owner hasn't explicitly server requests to be done over HTTPS.

Request made from curl with the -v tag

```
> curl -v https://www.worldql.com
*   Trying 172.67.190.57:443...
* Connected to www.worldql.com (172.67.190.57) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
*  CAfile: /etc/ssl/certs/ca-certificates.crt
*  CApath: none
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use h2
* Server certificate:
*  subject: C=US; ST=California; L=San Francisco; O=Cloudflare, Inc.; CN=sni.cloudflaressl.com
*  start date: Aug 30 00:00:00 2021 GMT
*  expire date: Aug 29 23:59:59 2022 GMT
*  subjectAltName: host "www.worldql.com" matched cert's "*.worldql.com"
*  issuer: C=US; O=Cloudflare, Inc.; CN=Cloudflare Inc ECC CA-3
*  SSL certificate verify ok.
* Using HTTP2, server supports multiplexing
* Connection state changed (HTTP/2 confirmed)
* Copying HTTP/2 data in stream buffer to connection buffer after upgrade: len=0
* Using Stream ID: 1 (easy handle 0x5646f608d9f0)
> GET / HTTP/2
> Host: www.worldql.com
> user-agent: curl/7.80.0
> accept: */*
>
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* Connection state changed (MAX_CONCURRENT_STREAMS == 256)!
< HTTP/2 200
< date: Fri, 31 Dec 2021 13:17:44 GMT
< content-type: text/html
< pragma: no-cache
< cache-control: no-cache
< cf-cache-status: DYNAMIC
< expect-ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
< report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=szoA4uvq0N3G%2FHXyOm77nqgzHlJhb9RxazppNlD5DWBe2cYEpOcmnpVymlWR2OpxhxnAbmCJaPVqSt7k3154nqPSDE0PruGmuFylTMyqjZWqrT1
< nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
< server: cloudflare
< cf-ray: 6c63ca305d521d95-BLR
< alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
<
* Connection #0 to host www.worldql.com left intact
<meta name="viewport" content="width=device-width,initial-scale=1.0,maximum-scale=1.0"/><style>body{margin:0px;padding:0px;}iframe{width:100%;height:100%}</style><iframe src="https://www.airtel.in/dot/" w
```

Partial Traceroute to the anycast server:

```
 4  125.21.18.205 (125.21.18.205)  17.621 ms 125.16.168.69 (125.16.168.69)  17.610 ms 125.21.20.121 (125.21.20.121)  11.307 ms
 5  182.79.141.70 (182.79.141.70)  74.631 ms 182.79.240.103 (182.79.240.103)  53.450 ms 116.119.61.183 (116.119.61.183)  53.439 ms

 6  182.79.164.25 (182.79.164.25)  54.442 ms 182.79.223.41 (182.79.223.41)  49.094 ms 182.79.164.25 (182.79.164.25)  55.140 ms
 7  104.21.92.184 (104.21.92.184)  60.631 ms  51.116 ms  48.306 ms
```

Impact

This not only gives the end user a false sense of security (seeing the HTTPS padlock) on Cloudflare served sites, it allows my ISP to serve ANYTHING over a HTTPS connection with a valid CA certificate on some cloudflare served sites, allows it to see the content in plain text. It actually defeats the whole point of TLS!

I understand that this can happen over on the origin end too, and there is no way to get around this without enforcing HTTPS to origin servers, but I'm really concerned with a active MITM of edge server, which I was led to believe was under secure network.

Activity

Hi @anunayj,

Thank you for your submission. I hope you are well. Your report is currently being reviewed and the HackerOne triage team will get back to you once there is additional information to share.

Have a great day!

Kind regards,
@princeofpersia

PrinceOfPersia	2022-01-04 14:57	comment	Public

Hi @anunayj,

I will check with the team regarding your report, I will let you know once we hear back from them.

Regards,
@princeofpersia

PrinceOfPersia	2022-01-04 15:07	comment	Public

Enabling SSL/TLS between Cloudflare and the origin site is a customer decision. When this protection is not enabled, as is the case here, an ISP can manipulate the requests before they reach Cloudflare. If this behaviour is not desired, the customer must change the settings for the site in the Cloudflare dashboard.

Lucas	2022-01-05 10:15	comment	Public
Lucas	2022-01-05 10:15	bug not applicable	Public
Chad Chalker	2022-02-01 01:06	reassigned to team	Public