Play the Opera Please

Play the Opera Please - Author not stated, inputzero.io.

- Published: date not stated
- Original: <https://www.inputzero.io/2021/04/play-the-opera-please.html>
- Preserved from: https://www.inputzero.io/2021/04/play-the-opera-please.html (live) on 2026-08-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

Prior approval are taken from Opera security team before disclosing this issue!

Before we get started there are few things which we need to understand such as,

Value added service (VAS): Value added services (VAS) is a popular telecommunications term for non-core services, example: (Caller-tunes, Missed call alerts, Online gaming etc).

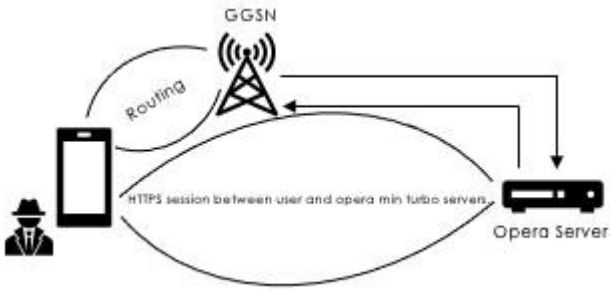
**GGSN: **The gateway GPRS support node (GGSN) is a main core component, GGSN is responsible for the interworking between the GPRS network and external packet, basically this is a routing device.

HTTP header enrichment (HE Process): HTTP header enrichment is the process of adding data fields in the HTTP header. This is commonly used in mobile networks by adding user and device identifiers in HTTP requests such as IMEI, IMSI, MSISDN or other data to identify subscriber or mobile device details[1].

As per my understanding during a VAS subscription process, GGSN picks up the MSISDN from HTTP header to subscribe end users, the idea is to abuse HTTP header enrichment process via Opera mini browser which could lead to fraudulent VAS activation.

Why Opera mini? Opera mini is famous for data compression (data saving mode) although it supports three types of data savings compressions modes. direct, extreme and high.

Once the request is initiated and routed by GGSN all communication happens in HTTPS, hence GGSN will not be familiar with the source MSISDN, because there is no header enrichment process, Opera turbo server establish a secure session to perform rest of the process during the subscription. In this case GGSN acts as a routing device and fails to perform HE process (Because HE can only be performed on HTTP protocol but Opera mini creates an HTTPS based session).



Post this if we navigated to https://www.inputzero.io snif the packets via wireshark the source IP would be our public IP and destination hits to opera turbo servers such as `*global-4-lvs-hopper.opera-mini.net*` rather than www.inputzero.io.

Having said that, after countless assessment on the subscription process via opera mini, I found one `ping` request which is generated via opera mini, when its is open for the first time after clearing the cache and temp data of the browser. It was observed, that ping request is responsible for taking MSISDN and creating the session for entire flow.

Injecting MSISDN headers in this request with the victims MSISDN, the session was established by victims number with opera turbo server and now you can impersonate victim and subscribe for any VAS service to deduct his/her digital money. With a successful subscription using the above steps and server log it was concluded that opera turbo servers don't validate/filter certain injected HTTP headers which leads to activation of VAS services.

Patch: Opera turbo stops forwarding such injected HTTP headers and CVE-2018-19825 was assigned to this which states "Lack of filtering of certain HTTP headers could lead to fraudulent VAS activation."
