Document 3

EUROPEAN COMMISSION

DIRECTORATE-GENERAL FOR INFORMATICS

WiFi4EU – Consolidated technical report

[DG CONNECT – System owner].

Prepared by: [redacted]

13/06/2018

1. CONTEXT

On Tuesday 15 May the Commission was alerted of two vulnerabilities affecting the WiFi4EU grant application service:

1) A vulnerability could potentially impact the timestamping of applications for vouchers. This is important because the grants are available on a first come first served basis. After checking, it was discovered that the initial suspicion of a vulnerability (the ability to tamper with the timestamp on the central server) was not correct and an accurate record of the actual time of application has been established.

However during this investigation a functional flaw was discovered as the enabling of the "Apply" button on the screen of the applicant was based on the applicants own computer clock rather than on the central server clock (our reference). Thus depending on the own applicants clock, the applicant has either been able to apply before the 13.00 CEST (i.e. the legal start-time) or has been prevented to apply at the 13.00 CEST sharp. There is no indication that there was any malicious exploitation of this functional flaw.

2) An access control vulnerability could potentially permit users of the service to gain visibility on information of registered applicants and suppliers including personal data (names, job titles, scanned copy of passports and ID cards -including signatures-, addresses, phone numbers). This vulnerability was found to be valid and has triggered a detailed investigation of logs to examine if this potential data exposure has enabled illegal access to personal information potentially consisting in a data breach. Based on the evidence found, a separate report on data security (drafted as of June 12, 2018 by Ken Ducatel, to be finalised and filed) concludes that there is no sign of massive export of private data or of accesses consistent with a concerted attack leading to a data breach

This report aims at clarifying the nature and extent of the technical faults detected at the launch of the 1st WiFi4EU call, including addressing additional interrogations from CNECT on the possibility to alter the apply button (to enable it) and regarding the mechanism to process the application requests.

This report will therefore focus on describing the following:

- Functional flaw on the clock synchronisation
- Further potential manipulation of the apply button
- Access control vulnerability
- Technical Solution to process the application requests

2. FUNCTIONAL FLAW ON THE CLOCK SYNCHRONISATION

The enabling of the "Apply" button on the screen of the applicant was based on the applicants own computer clock rather than on the central server clock (the European Commission reference). Thus depending on the applicants own clock, the applicant has either been able to apply before the 13.00 CEST (i.e. the legal start-time) or has been prevented to apply at the 13.00 CEST sharp.

Several solutions have been identified to solve this flaw and are being considered for the re-opening of the portal.

3. FURTHER POTENTIAL MANIPULATION OF THE APPLY BUTTON

In addition to the point 2 (Functional flaw on the clock synchronisation), the possibility of manipulating the apply button to enable it before 13.00 existed. It could be done by modifying locally the script/code source on the computer of the applicant (not on the Commission sever). This manipulation could be done only intentionally and would have generated an application before 13.00 (i.e. invalid application). This information was known before the call by all stakeholders however it was not considered as an issue for the reasons mentioned above.

4. ACCESS CONTROL VULNERABILITY

An access control vulnerability in the WiFi4EU system could potentially permit users of the service to gain visibility on information of registered applicants and suppliers including personal data (names, job titles, scanned copy of passports and ID cards -including signatures-, addresses, phone numbers). As detailed in a separate security report (drafted as of June 12, 2018 by Ken Ducatel), there is no sign of massive export of private data or of accesses consistent with a concerted attack leading to a data breach.

This vulnerability has now been corrected and will be further validated after a full security scan.

5. TECHNICAL SOLUTION TO PROCESS THE APPLICATION REQUEST

The “first come, first served” principle as requested by the legal basis of WiFi4EU implies that the WiFi4EU system needed to be capable of handling more than 10.000 requests in just a few seconds while guaranteeing the order of arrival. The WiFi4EU system relies on a secure queue in order meet these very specific requirements.

Once the apply request is received at the Commission servers, the secure queue preserves the order of arrival and guarantees a reliable timestamp. The timestamp is accurate up to the level of nanoseconds and is independent from the applicants clock. There is no possibility to alter this information once the messages arrive at the Commission controlled infrastructure. However, the system cannot guarantee that the order of arrival in our server is exactly the same as the order of actual clicking by all applicants, due to the inherent uncertainty of technical latency issues.

As a side-effect of using the queue mechanism, a registered user can open multiple browsers and therefore repeat his/her application for the same municipality until the queue is treated. This constraint was accepted by CNECT, and it was decided to take into account only the first application while discarding the others for the same municipality. Transferring the information from the queue to the WiFi4EU database implies a delay which was also accepted by CNECT.

This technical solution proved to be successful as the WiFi4EU system was able to handle the heavy load impose by the opening of the call.

6. FURTHER ACTIONS TOWARDS THE CONTRACTOR

The contractor holds the main responsibility of the defects of the delivered software. A discussion with our contractual unit is going-on at the moment to propose measures at that level.

OUT OF SCOPE

7. LESSONS LEARNT

Like any IT projects, WiFi4EU involves multiple stakeholders. Each of them have specific roles and responsibilities in their domain (business, IT, project management, etc.). A complete lessons learnt exercise should be performed with all stakeholders in order to implement a comprehensive set of counter-measures in place for all issues identified in this exercise.

It is already clear that measures should be put in place to enforce quality, functionalities, performance and security and that each stakeholder has a role to play in this framework. As an example, all stakeholders should commit to the 6 weeks period to test (functionality, performance and security) after the first delivery of a major functionality.