EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR INFORMATICS

WiFi4EU – 15 May 2018 Security Incident Report

Prepared by: DG INFORMATICS

- **CONTEXT**

On Tuesday 15 May 2018, the Commission was alerted by an IT company of two potential vulnerabilities affecting the WiFi4EU grant application service (online portal www.wifi4eu.eu). After a first rapid plausibility check with the source of the information, the Commission services decided to suspend the functioning of the online portal in order to prevent any possible damage to citizens data and/or to the integrity of the call for applications.

- **INVESTIGATION SCOPE AND RESULTS**

The issues raised were the following:

1) a suspicion that a vulnerability could potentially impact the timestamping of grant requests. This is important because the grants are allocated on a first come first served basis. After checking, the Commission determined that this initial suspicion was not confirmed and that an accurate record of the actual time of each application had been established. The Commission concluded that there had been no manipulation of the data in the WiFi4EU portal.

The investigation revealed a different issue: due to a functional flaw, the ability for applicants to use the "Apply" button was based on the applicant's own computer clock rather than the central server clock (the reference for the call procedure). Thus, depending on the own applicant's clock, certain applicants were able to apply in good faith before the 13:00 CEST (the legal start-time) and others were prevented from applying at 13:00 CEST sharp. This flaw is not linked to differences in time zones. There is no evidence that early applicants changed this clock setting on their PC on purpose, and it is impossible to identify applicants who may have been artificially constrained from applying on time.

This functional flaw will be corrected before the launch of the next call for applications.

2) An access control vulnerability could potentially permit users of the service to gain visibility on information or download documents of other registered applicants and Wi-Fi installation companies including personal data, such as contact details and proof of identity. This vulnerability was found to be valid and has triggered a detailed investigation to examine whether, beyond activity linked directly to the detection of the vulnerability, this potential data exposure had been exploited by third parties. The analysis of the available data revealed only minimal data access with no evidence of malicious intent. Data protection compliance steps have been taken accordingly.

This vulnerability has been corrected. Additional full security scans will be performed before the portal is activated for registrations prior to the next call.

- **CONCLUSION**

After a thorough analysis, the Commission concludes that, as far as security is concerned, there has been no manipulation of the data in the WiFi4EU portal, nor evidence of any malicious access to the data stored in the system.

The functional flaw revealed by the investigation will be corrected before the launch of the 2nd call. The Commission will re-open the online portal only after a full security scan is carried out. The portal will resume its operation well before the 2nd call for applications is opened.