The Computer Emergency Response Team of the EU Institutions, Bodies and Agencies (CERT-EU) is aware that 14 Institutions, Bodies or Agencies (EUIBAs) use SolarWinds Orion product, and that at least 6 of them have been affected by the hack. For those affected, the level of compromise varies significantly, from no impact to significant impact.

Incidents and other relevant data are reported to CERT-EU on a voluntary basis. Given that the affected EUIBAs sent limited details on the attack and that the logs are often not available, CERT-EU can provide only limited information. In some cases, IT networks and systems have been significantly impacted, and at least some personal data breaches occurred. Mitigations depend on the cases and are proportional to the risk and the specific findings. Examples of mitigation include re-installing SolarWinds servers, changing passwords, network architecture and configuration.

Moreover, as soon as the attack was discovered on 13 December 2020, CERT-EU immediately released a threat alert, with actionable information to detect and mitigate possible infections. Since then, five updates of this threat alert were released. Overall, CERT-EU assesses that the attempts have been successfully contained and continues to actively work with the EUIBAs to respond to the incident.

CERT-EU investigates incidents as they are detected or reported by EUIBAs. Since 1 December 2020, around 200 incidents, of different severity, were investigated; only one was related to SolarWinds.

CERT-EU is obliged to keep the identity of the impacted EUIBAs secret, unless specifically authorised by the affected party. It is not possible to disclose additional details of the investigations.