Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:121 **15-12-2020**

Subject: SolarWinds Orion platform software updates recently Hacked

Known Affected Products: Orion Platform versions **2019.4 HF 5** and **2020.2 with no hotfix or with 2020.2 HF 1.**

Summary:

It has been recently reported that a software of technology company "**SolarWinds**" Orion software had been hijacked by highly sophisticated malicious actors to break into thousands of its users, **which downloaded the SolarWinds Orion compromised software update**. The downloaded update allowed the hackers to spy unnoticed on affected organizations and agencies.

For further details, please visit following official link:
https://www.solarwinds.com/securityadvisory

Recommendations:

- It is highly recommended that users should upgrade to Orion Platform version **2020.2.1 HF1** as soon as possible,by accessing https://customerportal.solarwinds.com/, where all of the updated versions are available.
- SolarWinds has recommended that all users should update to release **2020.2.1 HF2,** once it is available, as the 2020.2.1 HF2 release replaces the compromised component and will also provide several additional security enhancements, in the product.

- In case of any difficulty, please follow the guidelines available at below official link for securing Orion Platform instance:
  https://documentation.solarwinds.com/en/Success_Center/orionplatform/content/core-secure-configuration.htm

- Primary mitigation steps also include having your Orion Platform installed behind firewalls, disabling internet access for the Orion Platform, and limiting the ports and connections to only what is necessary.
- Always update all software including Operating Systems, Servers, web browsers etc. to the latest and stable versions with appropriate patches.
- Whenever required, access the system with minimal access rights and privileges.
- Maintain and implement a strong password policy throughout the infrastructure.
- Install, regularly maintain and update Antivirus solution from a well reputed vendor.
- Regularly provide Cyber security awareness trainings to the employees.
- Do not download attachments from emails unless they are from the trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.