TLP: White[1]

Advisory- SolarWinds Orion Platform Compromise

Dear Constituents,

As you are aware SolarWinds has been a victim of a vulnerability that was inserted into their Orion Platform software builds for versions 2019.4 HF 5, 2020.2 with no hotfix installed, and 2020.2 HF 1. The vulnerability was inserted as a result of a cyberattack on SolarWinds.

How it Works

The vulnerability introduces a backdoor remote execution access to servers running the vulnerable versions. A sophisticated threat actor has been using this access to compromise networks and ex-filtrate data, with high-profile compromises reported in government departments and companies in the United States. The nature of this vulnerability means any organisation using these versions could be affected or is likely vulnerable to exploitation.

For a complete list of the affected products, please refer to the below link under References

What to do

1. It is recommended to immediately isolate any Orion server from the network and apply the hotfix, released by SolarWinds- Orion Platform version **2020.2.1 HF 1**
2. Apply the subsequent hotfix **2020.2.1 HF 2** which replaces the compromised component and provides several additional security enhancements.
3. If you have been affected by this, we would urgently like to hear from you.

References

- https://www.solarwinds.com/securityadvisory
- https://www.solarwinds.com/certadvisory

1 CERT Tonga adopts the Traffic Light Protocol

Please for more information contact us:

CERT Tonga
Ministry of MEIDECC
Nuku'alofa
Tel: 2378 (CERT) or (+676)20-101
email: cert@cert.gov.to
web: www.cert.gov.to
Twitter: @CERTTonga | Facebook: @CERTTonga

Disclaimer Notice:

The information in this notice is intended solely for public knowledge and awareness, and not intending to harm, fright or disturb any person(s), legal entity or the receiver of this information. Under no circumstances shall the Ministry of MEIDECC be liable for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with your access or use of or inability to access or use the information and any third party content and services