ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

NOTE DE SECURITE

Titre	Malware affectant certaines versions de la plateforme SolarWinds Orion
Numéro de Référence	28121512/20

Produits affectés

Les produits de la Plateforme SolarWinds Orion versions 2019.4 HF 5 et 2020.2 SANS hotfix ou 2020.2 HF 1 :

- Application Centric Monitor (ACM)
- Database Performance Analyzer Integration Module (DPAIM)
- Enterprise Operations Console (EOC)
- High Availability (HA)
- IP Address Manager (IPAM)
- Log Analyzer (LA)
- Network Automation Manager (NAM)
- Network Configuration Manager (NCM)
- Network Operations Manager (NOM)
- Network Performance Monitor (NPM)
- NetFlow Traffic Analyzer (NTA)
- Server & Application Monitor (SAM)
- Server Configuration Monitor (SCM)
- Storage Resource Monitor (SCM)
- User Device Tracker (UDT)
- Virtualization Manager (VMAN)
- VoIP & Network Quality Manager (VNQM)
- Web Performance Monitor (WPM)

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Résumé

SolarWinds annonce la découverte de la compromission de certaines versions de sa plateforme de supervision SolarWinds Orion (2019.4 HF 5 and 2020.2 sans hotfix ou 2020.2 HF 1) par du code malicieux.

Les attaquants ont pu compromettre la chaine d'approvisionnement de mises à jour en y incluant un « Backdoor» nommé « SUNBURST» pour par la suite effectuer d'autres types d'attaques comme l'exécution de code ou l'exfiltration de données sensibles.

Selon Fireye, cette campagne qui a commencé au printemps de 2020 aurait ciblé et cible encore plusieurs grandes entités dans le monde.

Solution

Dans le cas où vous utilisez la plateforme SolarWinds Orion Il est recommandé de :

- Isoler les serveurs contenant une version vulnérable de SolarWinds Orion
- Investiguer si votre système d'information a été compromis en se basant sur les indices de compromission publiés par Micorsoft et Fireye
- Mettre à jour votre plateforme SolarWinds Orion

Références

Note de sécurité de SolarWinds :

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

Rapport de FireEye :

- https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

Indicateurs de compromission publiés par FireEye :

- https://github.com/fireeye/sunburst_countermeasures/tree/main/indicator_release

Guide d'investigation publié par Microsoft :

- https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma