ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Deuxième Malware affectant SolarWinds Orion
Numéro de Référence	28252512/20
Date de Publication	25 Décembre 2020
Risque	Critique
Impact	Critique

Systèmes affectés

Veuillez-vous référer au bulletin de sécurité de Solarwinds pour trouver les versions affectées.

Bilan de la vulnérabilité

SolarWinds annonce la découverte d'un nouveau malware nommé « SUPERNOVA » qui est distribué par le biais d'une vulnérabilité affectant plusieurs versions de SolarWinds Orion.

Ce Malware qui consiste en un « Web Shell » s'exécute dans la mémoire du serveur vulnérable pour permettre aux attaquants d'exécuter du code, d'exfiltrer des données confidentielles ou d'effectuer d'autres activités malicieuses.

Solution

Veuillez-vous référer au bulletin de sécurité de SolarWinds pour installer les mises à jour.

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – 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 ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risques

- Exécution de code arbitraire.
- Accès à des données confidentielles

Références

Bulletin de sécurité de de SolaWinds du 24 Décembre 2020 :

- https://www.solarwinds.com/securityadvisory#anchor2

Rapport de Palo Alto détaillant le mode de fonctionnement et les IOC pour la détection de « SUPERNOVA » :

- https://unit42.paloaltonetworks.com/solarstorm-supernova/