SolarWinds Hackers "Impacting" State and Local Governments

Via Infosecurity - Latest News

SolarWinds Hackers « Impacting » État et les gouvernements locaux

L'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a lancé un avertissement sur l'impact généralisé d'une récente attaque de piratage informatique qui a compromis la chaîne d'approvisionnement des logiciels SolarWinds Orion.

L'assaut sur SolarWinds a fait les manchettes plus tôt ce mois-ci après qu'il a été découvert et divulgué par les chercheurs de FireEye. Le groupe avancé de menaces persistantes (APT) à l'origine de l'attaque a réussi à compromettre les organismes gouvernementaux, les infrastructures essentielles et les organisations du secteur privé.

Consciente de la gravité de l'attaque, la CISA a présenté le 13 décembre une directive d'urgence appelant « tous les organismes civils fédéraux à revoir leurs réseaux à la recherche d'indicateurs de compromis et à déconnecter ou à alimenter immédiatement les produits SolarWinds Orion ».

Mercredi, l'agence a décrit la campagne omniprésente comme un « incident cyber important » et a déclaré qu'elle affecte le gouvernement américain à tous les niveaux.

Dans une déclaration publiée sur son site Web, l'agence a déclaré qu'elle « suit un incident cybernétique important qui a un impact sur les réseaux d'entreprises dans les gouvernements fédéral, étatiques et locaux, ainsi que sur les entités d'infrastructure essentielle et d'autres organisations du secteur privé ».

CISA a déclaré que l'acteur APT responsable de compromettre la chaîne d'approvisionnement des logiciels SolarWinds Orion a également effectué un abus généralisé des mécanismes d'authentification couramment utilisés et dispose de ressources suffisantes.

L'agence a ensuite averti les organisations de se concentrer sur la gestion de la menace posée par cette campagne particulière avant de s'attaquer à d'autres problèmes de cybersécurité.

« Cet acteur de la menace dispose des ressources, de la patience et de l'expertise nécessaires pour accéder à des

informations hautement sensibles si rien n'est fait », a averti l'agence.

« L'ACSA exhorte les organisations à donner la priorité aux mesures visant à identifier cette menace et à y faire face. »

L'agence s'est associé au Federal Bureau of Investigation (FBI) et au Bureau du directeur du renseignement national (ODNI) pour former un Groupe de coordination cyber unifiée (UCG) qui coordonnera une réponse de l'ensemble du gouvernement à l'attaque de SolarWinds.

L'ACSA a indiqué qu'il demeure disponible pour aider les organismes victimes de l'incident.

L'agence a déclaré qu'elle « reste en contact régulier avec les parties prenantes des secteurs public et privé et les partenaires internationaux, fournissant une assistance technique sur demande et mettant à disposition des informations et des ressources pour aider les personnes touchées à se remettre rapidement des incidents liés à cette campagne ».