DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 06-02-2023

BULLETIN ALERTES

Object	Campagne d'exploitation d'une vulnérabilité VMware ESXi
Réference	1026
Date de Publication	2023-02-05
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance

SYSTÉME AFFECTÉ :

ESXi versions 7.x antérieures à ESXi70U1c-17325551

ESXi versions 6.7.x antérieures à ESXi670-202102401-SG

ESXi versions 6.5.x antérieures à ESXi650-202102101-SG

DÉSCRIPTION :

Une campagne d'attaque a été découverte sur Internet. Celle-ci impliquant une vulnérabilité affectant le service Service Location Protocol (SLP) connues sous Vmware (CVE-2021-21974) qui permet à un attaquant distant d'exécuter du code arbitraire dans le but d'y déployer un Rançongiciel.

SOLUTION :

DJ-CERT recommande d'appliquer l'ensemble des correctifs de sécurité pour l'hyperviseur Exsi en prenant des mesures délicates afin de garantir la continuité du service. Néanmoins cette mesure ne suffisant pas dans le cas où le système est déjà compromis, l'analyse des systèmes est fortement recommandée pour recherche toutes forme de compromission.

CONTOURNEMENT PROVISOIRE :

L'éditeur dans son bulletin de securite propose un contournement qui consiste à désactiver le service SLP sur les hyperviseurs Esxi susmentionné.

DOCUMENTATION :

- Bulletin de sécurité VMware 23-02-2021
  https://www.vmware.com/security/advisories/VMSA-2021-0002.html
- Avis de sécurité CERT-FR CERTFR-2021-AVI-145 du 24 février 2021
  https://www.cert.ssi.gouv.fr/avis/CERTFR-2021-AVI-145/
- CVE-2021-21974
  https://www.cve.org/CVERecord?id=CVE-2021-21974
- Procédure permettant de désactiver le service SLP
  https://kb.vmware.com/s/article/76372