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	Exploitation active de la vulnérabilité RCE affectant HPE OneView
Numéro de Référence	60131901/26
Date de Publication	19 Janvier 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- HPE OneView - Toutes les versions antérieure à v10.20 ;

Identificateurs externes

- CVE-2025-37164;

Bilan de la vulnérabilité

Une campagne d'exploitation massive cible actuellement la vulnérabilité critique « CVE-2025-37164 », affectant HPE OneView, la plateforme de gestion de datacenters de Hewlett Packard Enterprise et ayant fait l'objet du bulletin de sécurité n°59441812/25. Cette vulnérabilité permet une exécution de code à distance (RCE) et est exploitée à grande échelle par le botnet RondoDox, selon les observations directes de Check Point Research.

RondoDox cible principalement les systèmes exposés sur Internet, tels que les serveurs web, les équipements réseau et les dispositifs IoT, afin de constituer de vastes réseaux de bots utilisés pour mener des attaques par déni de service distribué (DDoS), des opérations de minage de cryptomonnaies et le déploiement de malwares supplémentaires. Le botnet est déjà connu pour avoir exploité d'autres vulnérabilités critiques récentes, notamment React2Shell (CVE-2025-55182).

Solution

- Appliquer immédiatement les correctifs HPE pour OneView ;
- Appliquer des restrictions d'accès et filtrage réseau pour limiter les connexions aux seules sources fiables ;

- Surveiller les journaux et les activités anormales sur les systèmes OneView ;

Risque

- Exécution du code arbitraire à distance ;

IOCs :

- 192.159.99.95
- 41.231.37.153
- cf90636d7794561da9743a249aa7dbaaa17612700b472f63d6de28930b559b84

Référence

Bulletin de sécurité maCERT/DGSSI du 18 Décembre 2025**:**

- https://www.dgssi.gov.ma/fr/bulletins/vulnerabilite-critique-affectant-hpe-oneview-software

Bulletin de sécurité Hewlett Packard Enterprise du 16 Décembre 2025**:**

- https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US#vulnerability-summary-1

- https://blog.checkpoint.com/research/patch-now-active-exploitation-underway-for-critical-hpe-oneview-vulnerability/