QUALYS®
CONTINUOUS SECURITY

Bulletin de sécurité - Alerte

Qualys publie un bulletin de sécurité pour la vulnérabilité « GHOST » découverte sur les systèmes Linux

Cette vulnérabilité sévère détectée dans la bibliothèque C de GNU/Linux donne le contrôle aux attaquants sans nécessiter d'identifiants système.
- Patchs disponibles dès aujourd'hui -

REDWOOD CITY (Californie) — Le 27 janvier 2015 — Qualys, Inc. (NASDAQ : QLYS), le principal fournisseur de solutions de sécurité et de conformité dans le Cloud, annonce que son équipe chargée de la recherche en sécurité a découvert dans la bibliothèque C de GNU/Linux (glibc) une vulnérabilité critique qui permet aux pirates de prendre le contrôle à distance de tout un système, en se passant totalement des identifiants système. Qualys a travaillé de manière étroite et coordonnée avec les fournisseurs de distributions Linux pour proposer un patch pour toutes les distributions de systèmes Linux touchés. Ce patch est disponible dès aujourd'hui auprès des fournisseurs correspondants.

Baptisée GHOST (CVE-2015-0235) parce qu'elle peut être déclenchée par les fonctions gethostbyname et gethostbyaddr, cette vulnérabilité touche de nombreux systèmes sous Linux à partir de la version glibc-2.2 publiée le 10 novembre 2000. Les chercheurs de Qualys ont par ailleurs détecté plusieurs facteurs qui atténuent l'impact de cette vulnérabilité, parmi lesquels un correctif publié le 21 mai 2013 entre les versions glibc-2.17 et glibc-2.18. Malheureusement, ce correctif n'ayant pas été classé comme bulletin de sécurité, la plupart des distributions stables et bénéficiant d'un support à long terme ont été exposées, dont Debian 7 (« Wheezy »), Red Hat Enterprise Linux 6 & 7, CentOS 6 & 7 et Ubuntu 12.04.

Les clients Qualys peuvent détecter GHOST à l'aide de la signature QID 123191 fournie par le service Cloud Qualys Vulnerability Management (VM). Lorsqu'ils lanceront le prochain cycle de scan, ils obtiendront des rapports détaillés sur l'exposition de leur entreprise à cette vulnérabilité sévère. Ils pourront ainsi estimer son impact sur leur activité et suivre efficacement la vitesse de résolution du problème.

« GHOST expose à un risque d'exécution de code à distance qui rend l'exploitation d'une machine par un pirate terriblement enfantine. Il suffit par exemple qu'un pirate envoie un mail sur un système sous Linux pour obtenir automatiquement un accès complet à cette machine », explique Wolfgang Kandek, Directeur technique de Qualys, Inc. « Compte tenu du nombre de systèmes basés sur glibc, nous considérons qu'il s'agit d'une vulnérabilité sévère qui doit être corrigée immédiatement. La meilleure

marche à suivre pour atténuer le risque est d'appliquer un patch fourni par votre fournisseur de distributions Linux. »

Pour plus d'informations (dont un podcast) sur GHOST, suivez les échanges sur notre blog Laws of Vulnerabilities.

Ressources supplémentaires

- En savoir plus sur Qualys Vulnerability Management
- Suivez Qualys sur LinkedIn et Twitter

A propos de Qualys, Inc.

Qualys Inc. (NASDAQ : QLYS), est le principal fournisseur de solutions de sécurité et de conformité dans le Cloud avec plus de 6 700 clients dans plus de 100 pays, dont une majorité des sociétés présentes aux classements Fortune 100 et Forbes Global 100.

Qualys Cloud Platform et sa suite de solutions intégrée aident les entreprises à simplifier leurs opérations de sécurité et à réduire le coût de la conformité. Cette plate-forme délivre un service à la demande de renseignement sur la sécurité. Elle automatise le spectre complet de l'audit, de la conformité et de la protection des systèmes d'information et des applications Web. Fondée en 1999, Qualys a signé des accords stratégiques avec des fournisseurs de services d'infogérance (« managed services ») et des cabinets de conseil de premier ordre comme, Accenture, Accuvant, BT, Cognizant Technology Solutions, Dell SecureWorks, Fujitsu, HCL Comnet, InfoSys, NTT, Tata Communications, Verizon et Wipro. Qualys est également l'un des fondateurs de la Cloud Security Alliance (CSA) et du Conseil sur la cyber-sécurité.

Plus d'informations sur www.qualys.com

Contact Qualys – Marketing Communication
Emily Vergnes 01 41 97 35 82
evergnes@qualys.com

Contact presse – AL'X Communication
Véronique Loquet 06 68 42 79 68
vloquet@alx-communication.com