# Une faille zero day sur les serveurs Apache massivement exploitée

Une vulnérabilité critique autorise la prise de contrôle complète de serveurs Web Apache, un environnement largement déployé et notamment utilisés pas des banques, des agences gouvernementales et des grandes entreprises de l'Internet (selon Netcraft, Apache est exploité sur plus de 300 millions de serveurs web). La brèche de sécurité réside dans le framework d'application web Struts 2. Elle est relativement facile à exploiter à partir de l'analyseur (parser) Jakarta Multipart lors du chargement d'un fichier. Deux méthodes d'exploitations sont d'ailleurs publiquement disponibles aujourd'hui.

La fondation Apache à fourni un correctif lundi 6 mars. Mais force est de constater que la mise à jour (2.3.32 / 2.5.10.1 ou plus) très fortement recommandée est loin d'avoir été appliquée en temps utile. Et la communauté constate une montée inquiétante du volume d'attaques depuis 48 heures. *« Talos a observé une nouvelle vulnérabilité Apache qui est activement exploitée sur le terrain »*, constatent les chercheurs de la filiale sécurité de Cisco sur le blog de l'entreprise. Ils évoquent même *« un nombre élevé d'événements d'exploitation »*.

## Bloquer les firewall

Parmi les exploitations, Talos constate l'injection de code dans des pages web qui permet de bloquer les firewall protégeant le serveur affecté. Ce qui ouvre la voie à des attaques de plus grande ampleur. Les attaques incluent notamment des «videurs» (bouncers) IRC qui permettent de cacher les adresses IP au cours d'échange par messagerie instantanées, mais aussi des agents de déni de service (DoS) et autres scripts pour enrôler les serveurs dans un botnet (réseau de machines contrôlées par des pirates). *« Ce sont plusieurs des nombreux exemples d'attaques que nous observons et bloquons actuellement*, indique Nick Biasini de Talos. *Ils se répartissent en deux grandes catégories: le sondage et la distribution de logiciels malveillants. »*

Reste à savoir pourquoi le taux des attaques est monté en flèche ces derniers jours. Est-ce l'annonce du correctif qui a poussé les pirates à profiter des délais parfois long des mises à jour dans certains secteurs? Il se pourrait en effet que le risque n'ait par été pris très au sérieux. Bien que classée à un niveau « élevé » (High), la vulnérabilité référencée CVE-2017-5638 est décrite par le support d'Apache comme permettant « potentiellement » l'exécution de code à distance (*Possible Remote Code Execution)*. C'est d'autant plus possible que le bug est exploitable même si l'application web n'utilise pas la fonction de téléchargement de fichier. Et très dommageable.

---

**Lire également**
**Les sites cachés Tor exposés grâce au serveur Apache**
**L'UE va vérifier la sécurité de KeePass et HTTP Apache**
**Une faille JBoss ouvre la porte des serveurs au ransomware SamSam**

**Crédit Photo : Gelbstock-Shutterstock**