20 vulnérabilités critiques corrigées dans Magento

20 vulnérabilités critiques corrigées dans Magento

Magento, fournisseur de solutions e-commerce open source, a patché plusieurs vulnérabilités présentant un risque d'attaques dont certaines de type XSS. Plusieurs éditions des versions communautaire et entreprise sont concernées.

Les administrateurs de sites e-commerce sous Magento ont tout intérêt à faire preuve de grande vigilance. L'éditeur vient en effet de lancer plusieurs correctifs pour combler des vulnérabilités critiques dans plusieurs versions de ses produits. Parmi les failles recensées, l'une permet d'injecter du code Javascript dans un champ de mail pour mener des attaques de type cross-site scripting (XSS). Considérée par Magento comme critique, cette vulnérabilité permet de pirater le compte administrateur de la session. Elle affecte l'édition communautaire de Magento (antérieure à la v1.9.2.3), ainsi que l'édition entreprise (antérieure à la v1.14.2.3) de la solution e-commerce open source.

La salve de correctifs permet également de combler 19 autres failles (relatives notamment aux formulaires de commandes, headers des adresses IP client, téléchargement de fichiers, deni de service newsletter, contournement de captcha…) dont certaines concernent également les v2.x des versions communautaire et entreprise de Magento. Il s'agit des premières vulnérabilités de taille que Magento a rencontrées cette année. En 2015, l'éditeur avait dû faire face à plusieurs problèmes dont une vulnérabilité critique exploitée ayant affecté un grand nombre de sites e-commerce.

Réagissez à cet article