Bug Bounty : Microsoft 365 majore ses primes

Microsoft dit verser dorénavant jusqu'à 26 000 $ aux hackers éthiques pour la découverte de bugs « à fort impact » dans ses produits Office 365.

La majoration de récompenses « basées sur des scénarios » concerne les programmes de bug bounty dédiés à Dynamics 365, Power Platform et Microsoft 365.

Microsoft veut ainsi inciter les chercheurs en sécurité à se concentrer sur la découverte de vulnérabilités à plus fort impact sur la confidentialité et la sécurité des comptes clients.

500 à 26 000 dollars

Initialement, tous niveaux confondus, les primes variaient de 500 $ à 20 000 $.

Désormais, les primes peuvent augmenter jusqu'à 30% pour la soumission de certains scénarios d'usage éligibles. La découverte d'une faille d'exécution de code à distance exploitable à partir d'une entrée non fiable (CWE-94), par exemple, peut donner lieu à un bonus de 30% couplé à la prime générale (M365 Bounty).

Dans le cadre des programmes M365 Bounty et Microsoft Dynamics 365 & Power Platform Bounty, les primes varient donc à présent de 500 $ à 26 000 $. Des récompenses plus élevées sont possibles, la décision se faisant « à la seule discrétion » de Microsoft.

L'éditeur a fait un choix similaire l'an dernier pour Azure Bounty Program. Microsoft versant désormais jusqu'à 60 000 dollars pour la découverte de vulnérabilités cloud à fort impact.

Microsoft, qui publie un cycle de correctifs de sécurité chaque deuxième mardi du mois (Patch Tuesday), a tout intérêt à réviser à la hausse ses primes de chasse aux bugs.

Le Bug Bounty étant la méthode la plus courante pour travailler avec des « white hats » ou hackers éthiques compétents dans un cadre légal.

Or, selon une étude promue par la plateforme spécialisée HackerOne, un hacker éthique sur deux hésite encore à divulguer une faille identifiée du fait d'une précédente expérience négative (risque juridique) ou d'un manque d'appui de l'entreprise concernée.

Selon une autre analyse, celle de Guillaume Vassault-Houlière, CEO et cofondateur de YesWeHack : « la sécurité crowdsourcée s'affirme non seulement comme le moyen le plus efficace de découvrir des vulnérabilités, dans le code, mais aussi pour rassurer les utilisateurs sur la sécurité d'un produit ou d'un service et sur la confidentialité de leurs données ».

(crédit photo © Microsoft)