Le Bug Bounty de l'US Army trouve une faiblesse du réseau interne

L'armée américaine a partagé les résultats de son premier Bug Bounty, nommé « Hack The Army » qui s'est déroulé pendant 3 semaines. Ce concours avait débuté le 21 décembre dernier et constituait le second programme gouvernemental de ce type, après celui visant le Pentagone.

Et le moins que l'on puisse dire est que cette chasse aux bugs a été prolifique. L'armée américaine a reçu plus de 400 rapports de bugs dont 118 étaient uniques et opérationnelles. Les participants ayant trouvé ces derniers bugs, ont été récompensés à hauteur de 100 000 dollars. L'US Army a rappelé que 371 personnes ont participé au Bug Bounty dont 25 employés gouvernementaux et 17 provenant des rangs de la Grande Muette.

Le réseau interne du ministère de la Défense fragilisée

Pourtant, elle a partagé des détails sur deux vulnérabilités sur le site goarmy.com. Combinées, ces deux failles peuvent ouvrir l'accès, sans authentification, à un site interne du ministère de la Défense. « *Ils sont arrivés par un proxy ouvert, ce qui signifie que le routage n'avait pas été verrouillé comme il aurait dû l'être et un des chercheurs sans même le savoir, a pu accéder à ce réseau interne* », explique l'armée dans un message publié sur HackerOne, hébergeur du bug bounty. Elle ajoute : « *En soi, les vulnérabilités ne sont pas particulièrement intéressantes, mais quand elles sont combinées, cela devient vraiment très grave.* » Bien évidemment ces deux brèches ont été colmatées rapidement après leurs découvertes.

Éviter l'automatisation

Le message se poursuit en vantant l'importance des personnes qualifiées pour la recherche de bugs, plutôt que de confier cette tâche à des systèmes d'automatisation pour éliminer les vulnérabilités. Et cette recherche doit faire appel à un public plus large que les simples militaires ou les agents gouvernementaux. L'ancien secrétaire de l'Armée, Eric Fanning, expliquait en novembre dernier lors de la présentation de Hack The Army que « *l'Armée doit tendre la main aux groupes technologiques et aux chercheurs aguerris à la pénétration des réseaux informatiques normalement interdits d'accès. Habituellement, nous aurions évité ce genre de personnes* ».

La réussite de ce second programme pourrait donner des idées à d'autres administrations américaines. Il reste à savoir qu'elle sera la stratégie de la nouvelle administration de Donald Trump en la matière. A suivre…

A lire aussi :

Cybersécurité : une armée de 6000 hackers pour la Corée du Nord
Sécurité : l'Europe inclut un bug bounty à son audit logiciel