IoT : Microsoft offre 100 000 $ pour hacker Linux

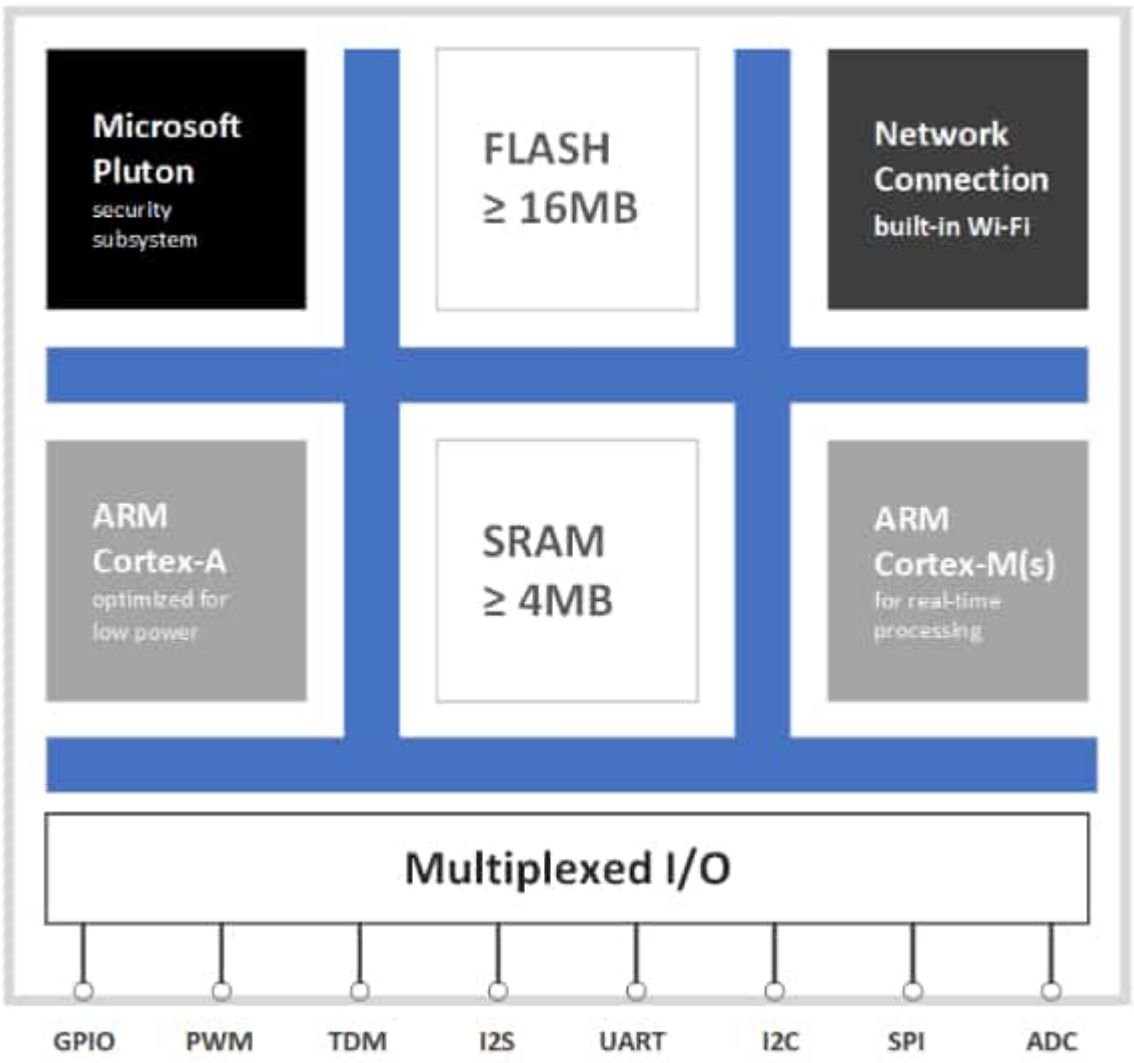
Les inscriptions à l'Azure Sphere Security Challenge sont ouvertes.

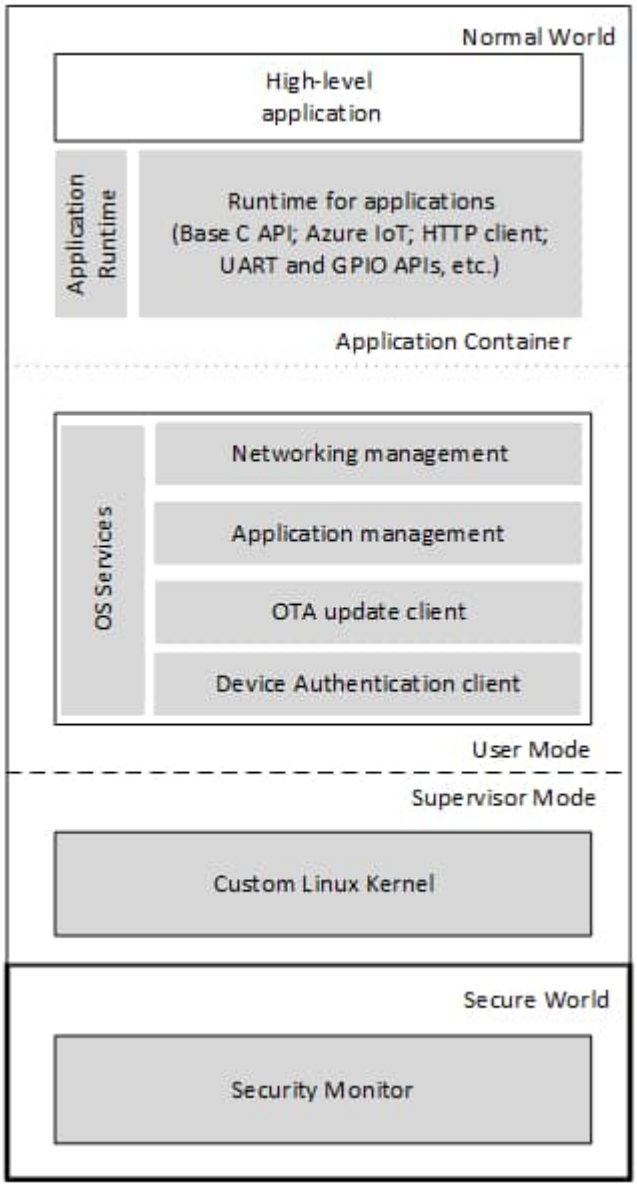
Microsoft donne jusqu'au 15 mai pour postuler à ce bug bounty à durée déterminée.

Les candidats retenus auront du 1er juin au 31 août pour signaler des failles dans la plate-forme IoT Azure Sphere, passée récemment en phase de disponibilité générale.

Ils pourront prétendre à la récompense maximale de 100 000 $ s'ils parviennent à compromettre l'un ou l'autre de ces éléments :

- Le sous-système de sécurité Pluton, intégré au microcontrôleur qui fait office de racine de confiance pour les objets connectés
- L'environnement Secure World, qui fait l'interface entre Pluton et le système d'exploitation Azure Sphere OS





Microsoft mettra des ressources à leur disposition dans le cadre du programme Azure Security Lab.

Les autres vulnérabilités éventuellement détectées sur Azure Sphere pourront donner lieu à des dédommagements axés sur la grille du bug bounty Azure. C'est-à-dire de 500 à 40 000 $, avec d'éventuels suppléments de 10 % pour une faille importante et 20 % pour une faille critique.

Sur cette liste d'« autres vulnérabilités » figurent par exemple :

- L'élévation de privilèges hors des conditions spécifiées dans le manifeste d'une application
- La modification des règles de pare-feu de sorte à accepter les communications sortantes vers des domaines non autorisés
- L'exécution de code non signé, à l'exception des techniques de type ROP

La partie services cloud d'Azure Sphere n'entre pas dans le cadre de ce bug bounty.

Illustration principale © Andrea Danti – Shutterstock.com