Sécurité serveurs : des ports USB virtuels mais des dégâts bien réels

À mesure que se développent les fonctionnalités d'administration à distance, la surface d'attaque s'élargit.

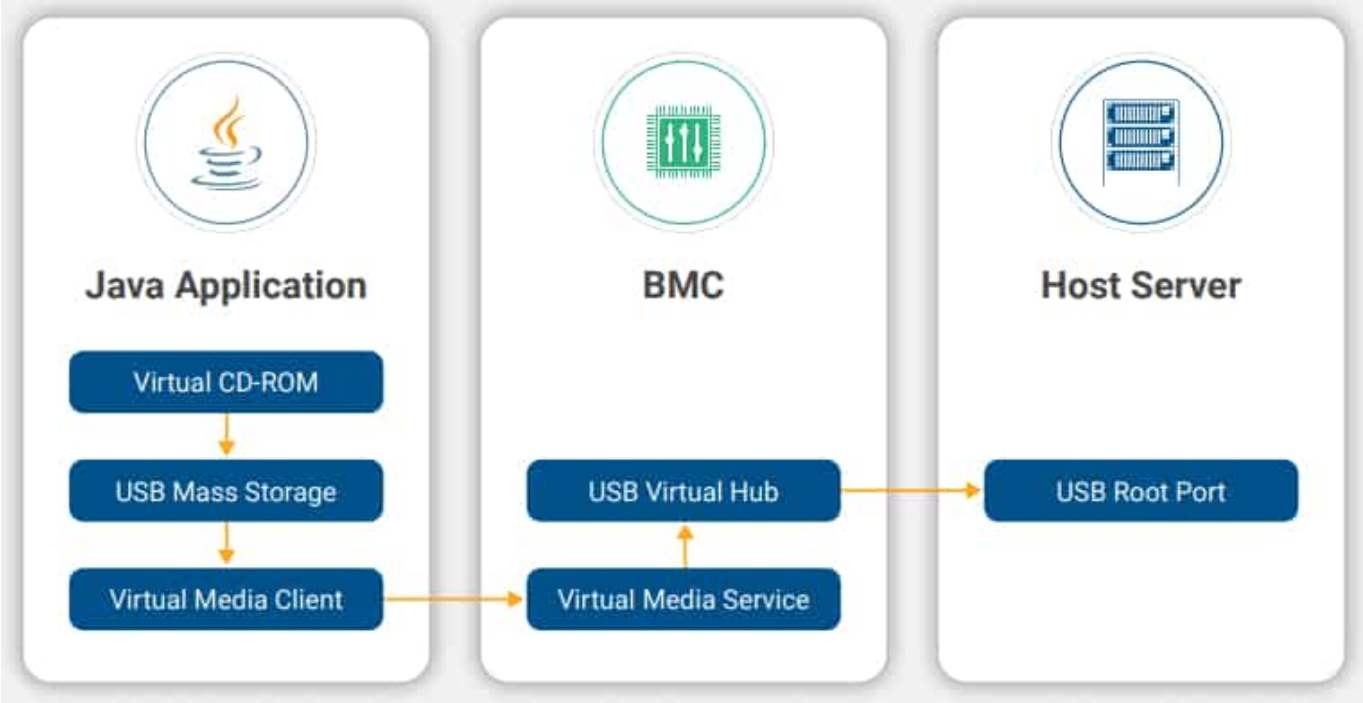
Les équipes d'Eclypsium l'ont souligné dans le cadre de l'Open Source Firmware Conference, qui se tient actuellement à Sunnyvale et Menlo Park (Californie).

Elles y ont présenté USBAnywhere, nom donné à un ensemble de failles dans les contrôleurs de gestion de la carte mère (BMC) sur certains serveurs Supermicro (plus précisément les plates-formes X9, X10 et X11).

Le point faible réside dans l'implémentation du service de média virtuel, qui donne accès à un concentrateur USB géré au niveau du BMC.

La connexion à ce service se fait par une application Java accessible sur l'interface d'administration du BMC. Mais plusieurs problèmes se posent :

- Les données d'authentification sont transmises en clair.
- Le trafic n'est pas chiffré aussi longtemps que le client ne le demande pas. Et lorsqu'il l'est, l'algorithme utilisé présente des faiblesses (il s'agit de RC4, banni notamment de TLS).
- Sur les plates-formes X10 et X11, on peut contourner l'authentification en exploitant la rémanence de certaines données après la déconnexion d'un administrateur.



À la carte

Une fois authentifié, le service de média virtuel permet de connecter jusqu'à 5 périphériques, de toute nature.

La démonstration d'Eclypsium se fonde sur le *framework* Facedancer, destiné à émuler des périphériques USB.
À partir de là, les possibilités sont multiples, de la solution clavier/souris à l'image disque malveillante.

Les chercheurs évaluent à près de 50 000 le nombre de serveurs Supermicro dont les BMC vulnérables sont exposés directement au réseau Internet.
C'est sans compter les serveurs isolés d'Internet, mais auxquels des tiers pourraient accéder en infiltrant des réseaux *corporate*.

Alerté le 19 juin, Supermicro vient de livrer un correctif. Une solution alternative consiste à bloquer le port TCP 623, ce qui désactivera le service de média virtuel.

Photo d'illustration © Supermicro