Quel est le spectre que votre VoIP s’effondre ?

Les systèmes de téléphonie, les SBC et le matériel VoIP qui reposent sur les processeurs Intel, AMD et ARM présentent de graves failles de sécurité

GAITHERSBURG, Maryland, le 11 janvier 2018 (GLOBE NEWSWIRE) – Patton Electronics, fabricant américain de solutions habilitantes UC, cloud et IoT pour les réseaux de transport, d'entreprise et industriels, déclare que les
systèmes d'exploitation Patton ne sont PAS vulnérables aux menaces de sécurité « Spectre » et « Meltdown
».*

Des rapports récents ont alerté le monde sur le fait que les périphériques construits sur Intel, Advanced Micro Devices (AMD) et Acorn RISC, ou les processeurs Advanced RISC Machine (ARM) plus récents, présentent des failles de sécurité importantes.

Les menaces Spectre et Meltdown permettent aux pirates informatiques d'accéder à toutes sortes d'éléments de réseau (et y faire des ravages), y compris les systèmes de téléphonie, les contrôleurs SBC (Session Border Controllers) et autres types de matériel VoIP, qui dépendent largement de ces processeurs.

Mais il y a une bonne nouvelle !

Les équipements client sur site (CPE) eSBC et VoIP SmartNode ne sont pas vulnérables à ces intrusions malveillantes. Donc, si vous avez choisi les solutions VoIP SmartNode de Patton, vous n'avez pas à vous inquiéter !

>>Lire l'avis officiel :

Patton Devices Not Vulnerable to Meltdown and Spectre Sidechannel Attacks

(Les périphériques Patton ne sont pas vulnérables aux attaques par canal auxiliaire Meltdown et Spectre)

L'équipe d'ingénierie avant-gardiste de Patton a mis en place une barrière autour du système

d'exploitation Patton. Cette « barrière » empêche les utilisateurs malveillants ou les logiciels tiers d'accéder au noyau.

Les bogues Spectre et Meltdown ne sont que les derniers ennemis que Patton a déjoués. Les produits Patton ont également protégé les clients contre les dangers tels que les bogues Heartbleed et Shellshock.

Un périphérique SmartNode sécurise la frontière entre les réseaux d'entreprise et du fournisseur de services. En plus d'être protégée elle-même contre les « Common Vulnerabilities and Exposures » (CVE) (failles et vulnérabilités communes), Patton a mis en place une large gamme de fonctionnalités de sécurité pour les réseaux voix et données convergés. Ces fonctionnalités incluent TLS/SRTP pour la voix et la signalisation codées avec une infrastructure à clés publiques (« Public Key Infrastructure » – PKI), plus un pare-feu intégré avec liste de contrôle d'accès (ACL) et une inspection avec état.

* Bien que Patton déclare que ses produits ne sont pas vulnérables aux menaces de sécurité Spectre et Meltdown, Patton ne fait aucune déclaration quant à la sécurité des éléments de réseau tiers. Patton recommande à tous les clients de suivre les conseils de tout autre fournisseur concernant la correction ou la mise à niveau de leurs produits et systèmes respectifs.

Contact presse : Glendon Flowers | +1 301 975 1000 |
press@patton.com
