Alerte chez CheckPoint, le Firewall-1 vulnérable?

Qualifiée de « highly critical » par Secunia, la faille de type « format string » vient d'être découverte dans le composant HTTP Security Server. Ce problème de sécurité pourrait permettre à un assaillant d'exécuter à distance du code arbitraire avec les droit « SYSTEM » ou « ROOT » ce qui lui permettrait de compromettre intégralement la sécurité du Firewall et donc du réseau que le Firewall protége.

Les versions affectées sont les suivantes : Checkpoint Firewall-1 NG-AI R55, R54, comprenant le SSL hotfix Checkpoint Firewall-1 HTTP Security Server comprenant NG FP1, FP2, FP3 Checkpoint Firewall-1 HTTP Security Server comprenant with 4.1 Le module « Application Intelligence (AI) » tient au c?ur du Firewall-1 un rôle de relais (proxy) dont le but est d'analyser les flux, détecter les anomalies, et bloquer certaines attaques potentielles. Ironie du sort c'est l'application HTTP embarquée qui permet l'administration à distance de ce module qui est vulnérable. La firme Israélienne met à disposition sur son site les correctifs nécessaires pour corriger cette faille sur vos équipements. **Aurélien Cabezon** Vulnerabilite.com (c)