10 juil 2020 -12:10

Le CCB met en garde contre une attaque potentielle de type ransomware

Le Centre pour la Cybersécurité Belgique (CCB) a reçu d'une source fiable des informations indiquant l'exploitation d'une vulnérabilité non identifiée dans les routeurs DrayTek, qui permet aux pirates informatiques à l'origine du ransomware d'accéder à des milliers de réseaux d'entreprise dans le monde entier.

Une étude du Centre pour la Cybersécurité Belgique (CCB) montre que les routeurs DrayTek Vigor2960 sont d'office touchés par la vulnérabilité non identifiée, tandis que d'autres appareils DrayTek risquent de l'être aussi.

La vulnérabilité permet aux pirates informatiques de contourner les procédures d'authentification et d'injecter ou d'exécuter un code à distance dans le système d'exploitation des routeurs DrayTek Vigor2960.

DrayTek a maintenant développé des correctifs pour certaines vulnérabilités de sécurité récemment divulguées, mais il reste difficile de dire si la vulnérabilité mentionnée ci-dessus a été corrigée. Le CCB recommande vivement aux utilisateurs d'installer les dernières mises à jour de sécurité sur les routeurs DrayTek.

Vérifier la présence éventuelle de portes dérobées

Le CCB a effectué des tests de pénétration qui ont montré que le correctif de la version 1.5.1.1 n'a pas éliminé les portes dérobées précédemment installées sur des routeurs DrayTek Vigor 2930 utilisant la version 1.4 du logiciel. Cela indique qu'un routeur compromis le restera même après la mise à niveau vers la version 1.5.1.1.

> « Nous appelons les entreprises à mettre à jour les appareils concernés et à vérifier les éventuelles portes dérobées. L'installation de la mise à jour de sécurité de DrayTek dans ce cas ne garantit pas que vous ne serez plus vulnérable à l'attaque de type ransomware potentielle. Si des pirates informatiques ont pu installer des portes dérobées avant la mise à jour, vous serez toujours vulnérable même après le correctif ».

Pedro Deryckere
Centre pour la Cybersécurité Belgique

Le CCB a averti ses parties prenantes à l'aide d'une alerte de sécurité spécifique reprenant la description, les conséquences potentielles et les solutions envisageables à la vulnérabilité et la menace.

Pistes d'action :

- Sauvegardez toujours votre configuration avant d'installer une mise à niveau.
- Mettez à jour vos appareils immédiatement et surveillez les nouveaux patchs disponibles pour les appareils DrayTek.
- Après la mise à niveau, veillez à vérifier que l'interface web affiche bien la nouvelle version du logiciel.
- Vérifiez qu'aucun profil d'accès à distance supplémentaire (connexion VPN, télétravailleur ou LAN to LAN) ou utilisateur admin (pour l'administrateur du routeur) n'a été ajouté.
- Vérifiez si des LCA (listes de contrôle d'accès) ont été modifiées.
- Désactivez l'accès à distance sur votre routeur si vous n'en avez pas besoin.
- Désactiver l'accès à distance (admin) et le VPN SSL. La LCA ne s'applique pas aux connexions VPN SSL (port 443). Vous devez donc également désactiver temporairement le VPN SSL jusqu'à ce que vous ayez mis à jour le logiciel.
- Activez le « syslog logging » pour surveiller les événements anormaux.

Le CCB a contacté et informé DrayTek, sans réponse.

Les ransomware, un phénomène en recrudescence

Un ransomware est un virus qui est installé sur un appareil sans le consentement de son propriétaire et qui exige une rançon en échange du déverrouillage de l'appareil et des fichiers.

Tout le monde peut être victime d'un ransomware : les particuliers, les travailleurs indépendants, les hôpitaux et même les grandes entreprises et le gouvernement.

Se protéger contre les ransomware

Pour tous les utilisateurs d'Internet :

- Il est crucial de protéger vos appareils avec un logiciel antivirus, mais une protection spécifique contre les ransomware est également devenue indispensable.
- De plus, il est toujours très important de reconnaître à temps les messages frauduleux et de régulièrement procéder à des mises à jour sur tous vos systèmes.

- Enfin, effectuez régulièrement des sauvegardes au cas où vous seriez victime d'un piratage informatique.

Pour les entreprises et les organisations :

- Les recommandations adressées à tous les utilisateurs d'Internet sont bien sûr également importantes pour les entreprises et les organisations, mais nous leur conseillons également d'aller plus loin.
- Pour les PME et les indépendants, un logiciel de protection des points terminaux peut être suffisant. Pour les grandes entreprises en revanche, une solution anti-ransomware spécialisée est recommandée.
- Mettez sur pied un plan de continuité et de reprise des activités avec un système de sauvegarde éprouvé.
- Assurez-vous que votre organisation est prête à faire face à une cyber-attaque. Consultez notre webinaire.
- Faites examiner par un spécialiste votre architecture et votre politique de sécurité informatique (y compris les politiques en matière de correctifs, de formation des utilisateurs, de segmentation du réseau, etc.)
- Travaillez sur une stratégie de cybersécurité. Lisez ici comment faire.

Les particuliers peuvent trouver tous les conseils dont ils ont besoin pour se protéger contre les ransomware sur le site www.safeonweb.be.

Les organisations et les entreprises peuvent consulter le site www.CERT.be. Nous avons publié le livre blanc « Ransomware : protection et prévention » en septembre 2019. Ce livre blanc a été mis à jour en 2020.

www.ccb.belgium.be

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - momenteel in verlof Eggers - momenteel in verlof
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be

© 2020 - news.belgium.be