PrintNightmare : cette faille qui menace Active Directory

Entre Stuxnet et PrintNightmare, quel rapport ? Le premier est passé à la postérité en mettant à mal, voilà plus de dix ans, des centrales d'enrichissement d'uranium en Iran. L'une des failles de sécurité qu'il avait exploitées résidait dans le spouleur d'impression Windows.

C'est ce même service qui pose problème avec PrintNightmare. La vulnérabilité a un identifiant (CVE-2021-34527), mais pas encore de correctif. En tout cas de la part de Microsoft. Son score de base sur l'échelle CVSS (8,8) reflète ses conséquences potentielles : l'exécution de code à distance avec des privilèges de niveau système.

On a connaissance de PrintNightmare depuis la semaine dernière… et cette erreur de la part des chercheurs qui l'avaient découverte. Ils ont en l'occurrence publié un PoC, croyant que Microsoft avait colmaté la faille. Le Patch Tuesday du 8 juin les a trompés. Il en élimine effectivement une de même nature (CVE-2021-1675).

> *Did you know Microsoft took one year to fix CVE-2021-1675 over and over ? Seems so hard for them to handle it correctly. I'll list the timeline here, have some lol or lqtm here. (A thread)*
>
> *— R3dF09 (@R3dF09) July 1, 2021*

Cette autre vulnérabilité, Microsoft l'avait d'abord décrite comme un levier d'élévation de privilèges. Le 21 juin, il en avait relevé le niveau de criticité, évoquant un risque d'exécution distante de code. C'est cette caractéristique qui a persuadé les chercheurs que leur PoC n'avait plus rien d'exclusif… et qu'ils pouvaient le publier.

Malgré le retrait ultérieur du PoC, le mal était fait.

> *We deleted the POC of PrintNightmare. To mitigate this vulnerability, please update Windows to the latest version, or disable the Spooler service. For more RCE and LPE in Spooler, stay tuned and wait our Blackhat talk. https://t.co/heHeiTCsbQ*
>
> *— zhiniang peng (@edwardzpeng) June 29, 2021*

PrintNightmare : recherche utilisateurs authentifiés

PrintNightmare s'enclenche par un appel à la fonction RpcAddPrinterDriver. En temps normal, elle permet d'ajouter des pilotes d'impression. Ici, elle ouvre la voie à l'injection d'une DLL vérolée.

Seul un utilisateur authentifié – ou, sur les contrôleurs de domaine, un utilisateur du domaine – peut invoquer la fonction. Microsoft liste les groupes dans lesquels on est susceptible d'en trouver. Et recommande deux options : désactiver soit le spouleur, soit l'impression distante.

Par défaut, les contrôleurs de domaine sont tous affectés, quelle que soit leur version de Windows. La raison : l'imbrication du groupe « Utilisateurs authentifiés » dans « Accès compatible pré-Windows 2000 ». Cette couche de compatibilité pour les systèmes Windows NT contient, en standard, des membres qui ont accès en lecture seule à tous les utilisateurs et à tous les groupes du domaine. Selon les paramètres définis à l'installation d'Active Directory, le groupe « Tout le monde » peut aussi y être imbriqué.

Les serveurs – hors contrôleurs de domaine – et les clients peuvent aussi se faire attaquer. Sous deux conditions. D'une part, que Point & Print soit activé. De l'autre, qu'« Utilisateurs authentifiés » soit imbriqué dans l'un des groupes sus-listés.

Le patch de juin semble fonctionner contre PrintNightmare. Y compris sur les contrôleurs de domaine, si on vide le groupe pré-Windows 2000.

> *Thanks to @_f0rgetting_ we have an explanation about why we have an Elevated Token (allowing #PrintNightmare on patched domain controllers): legacy*
>
> *If you remove « Authenticated users » from « Builtin\Pre-Windows 2000 Compatible Access », the original Microsoft Patch works again https://t.co/StvDdEWoog pic.twitter.com/h5IGJ0slpZ*
>
> *— Benjamin Delpy (@gentilkiwi) July 1, 2021*

Parmi les techniques alternatives, il y a la définition d'une règle interdisant l'accès au dossier des pilotes.

Illustration principale © A Stockphoto – Adobe Stock