SMB1 : une obsolescence délicate à gérer pour Microsoft

SMB1, bientôt exclu de Windows ? C'est plus compliqué qu'il n'y paraît. À la mi-avril, Microsoft a affirmé avoir enclenché la dernière phase de désactivation de cette version obsolète du protocole de partage réseau. Une édition du système d'exploitation est concernée : Famille. Sur les nouvelles installations, le client SMB1 n'est plus actif. On en a pour le moment un aperçu sur les canaux Dev et Bêta du programme Insider.

Voilà près de dix ans que Microsoft a officiellement déclaré SMB1 obsolète. Ses démarches s'étaient accélérées en 2017 après les épisodes WannaCry et NotPetya. Les deux *malwares* avaient exploité des failles inhérentes à ce protocole. À l'automne, avec la mise à jour Fall Creators Update, l'éditeur avait supprimé les parties serveur et client de SMB1 sur Windows 10 Entreprise, Éducation et Pro pour stations de travail. Ainsi que sur Windows Server 2019, alors encore en phase expérimentale. Sur les éditions Famille et Pro, le client restait installé, mais se désactivait automatiquement après 15 jours sans utilisation. L'année suivante, avec la version 1809 de Windows 10, le client avait aussi disparu de l'édition Pro. Là aussi, seulement pour les nouvelles installations.

Dans tous les cas, il reste possible de réinstaller SMB1, les fichiers (pilotes et DLL) étant pour l'instant toujours livrés avec le système. Microsoft envisage de les retirer, sans donner d'échéance. Il continuera toutefois à fournir, par après, un paquet d'installation externe, « sans support ».

> *There is still one thing left to do: stop including the SMB1 binaries at all. I'll talk more about this in a few months. I have a plan & the blog post above gives some details.*
>
> *— Ned Pyle (@NerdPyle) April 19, 2022*

SMB1 sur des routeurs, des NAS, des imprimantes…

Pourquoi ne pas couper totalement le cordon ? Parce que de nombreux équipements encore utilisés ont besoin de SMB1 pour fonctionner. Au fil des années, Microsoft a évoqué des NAS, des appareils médicaux, du matériel industriel, etc. Il a plus globalement recensé, à l'appui d'un hashtag et d'une adresse mail, une liste de produits concernés. À jour au 19 avril 2022, elle comprend des références d'une centaine de fournisseurs. On y trouve, entre autres :

– Côté **NAS**, du D-Link (série DNS), du Netgear (version antérieures à ReadyNAS OS 6), du QNAP (*firmware* antérieur au 4.1) et du WD (My Cloud Home, Wireless, Mirror, EX2) ; ainsi que Time Capsule d'Apple (qui semble ne pas pouvoir se connecter si SMB1 est désactivé)

– Parmi les **OS**, FreeBSD (<3.4 ; service smbfs), RHEL 5 et 6 (pour rejoindre des domaines), Solaris (11.3 et antérieures) et SUSE (11 et antérieures)

– De multiples **routeurs** dotés d'une fonction stockage USB (ASUS, Belkin, Huawei…) et plusieurs

modèles de passerelles réseau (Barracuda, Cisco…)

– Des **imprimantes** Epson (WF-3640, WF-5620…), Konica Minolta (BizHub, C284e, C3350…), Toshiba (E-Studio notamment), etc.

– Des **logiciels** comme NetServer (<V7R2) et QRadar (<7.3) chez IBM, Data Ingestor (<=6.4.0) chez Hitachi, ESXi (<6.0) chez VMware…

– Des caméras Axis, des baies de stockage Dell EMC… et même la Nintendo 3DS, qui utilise SMB1 pour gérer les microSD

Le statut de SMB1 sur ces produits n'est pas toujours – et de loin – officiellement documenté. Des sysadmins en ont par exemple témoigné sur Reddit. De leurs discussions ressortent quelques tuyaux : passage exclusif au FTP pour la sauvegarde de passerelles de sécurité, numérisation uniquement vers des adresses mail, etc.

Découverte réseau : Microsoft doit-il changer les choses sur Windows ?

Windows aussi a besoin de SMB1 sur certains aspects. En particulier la découverte du voisinage réseau. En tout cas avec la méthode « traditionnelle » : le service Computer Browser, intégré à l'explorateur et qui s'appuie sur NetBIOS. Avec la disparition de SMB1, Microsoft supprime aussi ce service. En guise d'alternative, il recommande FDPHost et FDResPub, qui utilisent WS-Discovery. Ou alors de mapper les ressources réseau.

Microsoft a publié un guide – assorti d'outils – pour aider, dans Windows, à la détection des ressources SMB1. À partir de Windows 8.1 et Windows Server 2012 R2, on peut supprimer le protocole. Sur les systèmes plus anciens, on ne peut que le désactiver. Si on remonte jusqu'à Windows XP (et Windows Server 2003), SMB1 doit être maintenu en fonction. Cela peut se révéler problématique sur les équipements qui utilisent version embarquée. Des utilisateurs en ont témoigné pour des machines de découpe laser Mitsubishi ou encore des fraiseuses à contrôleur Fanuc.

Par rapport à SMB1, SMB2 et SMB3 ont amélioré les performances du protocole (cache, leasing, agrégation de bande passante…). Sur le volet sécurité, ces versions ont notamment apporté :

– Des algorithmes plus robustes pour la signature des messages (MD5 dans SMB1 ; SHA-256 dans SMB2 ; AES-CMAC dans SMB3)

– Un contrôle d'intégrité préauthentification (les clés de session dérivent d'un hash, évitant les attaques qui reposent sur la manipulation des messages de négociation et d'initialisation de session)

Photo d'illustration © thodonal – Adobe Stock