VulnÃ©rabilitÃ© Microsoft Support Diagnostic Tool : RemÃ¨de
Suite Bureautique
PostÃ© par : JulieM
PubliÃ©e le : 7/6/2022 13:00:00

Une nouvelle vulnÃ©rabilitÃ© a rÃ©cemment Ã©tÃ© dÃ©couverte dans Microsoft Office. En effet, Microsoft Support Diagnostic Tool (MSDT) peut Ãªtre dÃ©tournÃ© contre les organisations. L'exploit semble exister depuis environ un mois, avec diverses modifications quant Ã ce qui doit Ãªtre exÃ©cutÃ© sur le systÃ¨me ciblÃ©.

Dirk Schrader, Resident CISO (EMEA) and VP of Security Research chez Netwrix, revient sur cette faille et comment la pallier :

Â« La vulnÃ©rabilitÃ© CVE-2022-30190 offre aux cybercriminels lâopportunitÃ© de dÃ©tourner les environnements informatiques des organisations via les terminaux. Cet exploit est susceptible de fonctionner sur la plupart des installations Windows et MS Office.

ConcrÃ¨tement, le hacker crÃ©e un document MS Word contenant le code malveillant, l'envoie Ã une adresse email professionnelle, puis utilise des techniques d'ingÃ©nierie sociale courantes pour inciter le destinataire Ã l'ouvrir.

Cette technique est possible car Word propose une fonctionnalitÃ©, appelÃ©e "modÃ¨le distant", qui est utilisÃ©e ici Ã mauvais escient pour obtenir un fichier HTML Ã partir d'un emplacement distant.Â

Une fois reÃ§u, ce fichier HTML utilise une fonctionnalitÃ© de MSDT pour exÃ©cuter une charge utile intÃ©grÃ©e, Ã l'aide d'un script Powershell ou d'autres outils disponibles sur la cible.

Or, les outils de sÃ©curitÃ© intÃ©grÃ©s de Windows ne dÃ©tecteront probablement pas cette activitÃ© et les tests de renforcement standard ne la couvrent pas. Un mÃ©canisme dÃ©fensif intÃ©grÃ©, comme Defender ou des restrictions courantes pour l'utilisation de macros, ne bloqueront pas non plus cette attaque.

Concernant les cibles, Microsoft rÃ©pertorie 41 versions diffÃ©rentes de produits touchÃ©es : de Windows 7 Ã Windows 11 ; de Server 2008 Ã Server 2022 ; Office, Office 2016, Office 2021 et Office 2022 sont Ã©galement concernÃ©s, quelle que soit la version de Windows sur laquelle ils s'exÃ©cutent. Des correctifs ont cependant Ã©tÃ© Ã©mis ces derniers jours.

Les premiÃ¨res dÃ©couvertes ont indiquÃ© que la suppression d'une clÃ© de registre empÃªcherait cet exploit de fonctionner, mais toutes les technologies de cybersÃ©curitÃ© ne couvrent pas ce paramÃ¨tre, nÃ©cessaire au processus de durcissement.

Pour dÃ©tecter les activitÃ©s suspectes liÃ©es Ã ce 0-day, les Ã©quipes informatiques doivent surveiller de prÃ¨s tout changement au sein des systÃ¨mes de leur organisation, en particulier dans les dossiers systÃ¨me, afin de repÃ©rer des processus ou services malveillants initiÃ©s.Â

Une autre mesure qui peut aider Ã prÃ©venir cette attaque consiste Ã Ã©tablir un ensemble de rÃ¨gles Windows qui verrouillent le systÃ¨me, ce qui empÃªche l'exploit d'exÃ©cuter la suite de lâattaque.

Dans les semaines Ã venir, les cybercriminels chercheront probablement des moyens de

militariser la vulnÃ©rabilitÃ©.Â

Ce 0-day dans le cadre dâ□□une campagne de spear phishing pourrait ainsi Ãªtre combinÃ© avec des vecteurs d'attaque innovants, ainsi que des techniques d'escalade de privilÃ¨ges, pour s'Ã©lever de la cible initiale.Â

Les professionnels de l'informatique doivent donc s'assurer que les systÃ¨mes sont Ã©troitement surveillÃ©s pour dÃ©tecter les activitÃ©s de compromission.

En outre, les groupes APT (Advanced Persistent Threat) et les cyber-escrocs devraient Ãªtre Ã la recherche des vulnÃ©rabilitÃ©s similaires, car elles facilitent lâ□□intrusion dans des systÃ¨mes informatiques. Â»