AYI NEDJIMI Consultants

PrintNightmare : Exploitation et Compron

20 April 2026 • Mis à jour le 20 April 2026 • 49 min de lecture

> Guide complet PrintNightmare (CVE-2021-34527) : exploitation Print Spoo
> opératoire pentest, détection et remédiation.

PrintNightmare demeure en 2026 l'une des vulnerabilites les plus emblematiques l'ecosysteme Windows. Regroupant les CVE-2021-1675 et CVE-2021-34527, cette Windows — un composant present par defaut sur chaque machine Windows depu elevation de privileges locale en SYSTEM ou une execution de code a distance av apres sa divulgation initiale, PrintNightmare continue d'etre exploitee activement c groupes d'attaquants avances, car de nombreuses organisations n'ont toujours pa service Print Spooler sur leurs controleurs de domaine. Cette analyse technique e d'exploitation, depuis la comprehension profonde du mecanisme vulnere jusqu'au compromission totale d'une foret Active Directory, en passant par les strategies d securite devrait implementer immediatement.

Contexte et chronologie : la confusion entre CVE-2021-1675 et CVE-2021-3452

Avant de plonger dans la chronologie des evenements, il convient de situer PrintN
vulnerabilites affectant le service Print Spooler de Windows. Ce service a fait l'obj
deux dernieres decennies. En 2010, Stuxnet exploitait deja une vulnerabilite du Pri
machines Windows. En 2020, CVE-2020-1048 demontrait qu'un utilisateur non pri
mecanisme de ports d'impression. Ces precedents auraient du alerter Microsoft s
service est reste fondamentalement inchange — un heritage technique dont les co
2021.

L'histoire de PrintNightmare est avant tout celle d'une confusion sans precedent d
amplifie considerablement l'impact de la faille et laisse des milliers d'organisations
comprendre l'ampleur du desastre, il faut remonter au Patch Tuesday de juin 2021
alors considere comme une simple elevation de privileges locale dans le service P
CVE-2021-1675.

Le 8 juin 2021, Microsoft attribue a cette vulnerabilite un score CVSS de 7.8 et la c
correctif est inclus dans les mises a jour cumulatives du mois de juin. A ce stade, l
faille serieuse mais geree de maniere routiniere. Personne ne soupconne encore q
mediatisees de la decennie.

Le tournant survient le 29 juin 2021, lorsque des chercheurs chinois de QiAnXin Te
accidentellement un exploit proof-of-concept fonctionnel sur GitHub. Les cherche
egalement le vecteur d'execution de code a distance qu'ils avaient decouvert inde
corrigeait que la composante LPE locale, laissant le vecteur RCE completement ou
heures, mais il est deja trop tard — le code a ete forke et distribue massivement a

Le 1er juillet 2021, Microsoft reconnait publiquement l'existence d'une vulnerabilite
attribue un nouveau numero CVE : CVE-2021-34527, avec un score CVSS de 8.8.
massive. Les administrateurs systeme qui pensaient avoir corrige la faille avec les