Vulnérabilité d'usurpation d'identité dans Windows LSA

Sur cette page

CVE-2021-36942
Faille de sécurité

Subscribe RSS PowerShell API

Date de publication : 10 août 2021

Assigning CNA: Microsoft

MitreCVE-2021-36942

Exploitabilité

Le tableau ci-dessous fournit une évaluation d'exploitabilité pour cette vulnérabilité lors de la publication initiale.

Publicly disclosed
Oui
Exploited
Non
Exploitability assessment
Exploitation plus probable

Forum aux questions

Comment un attaquant pourrait-il exploiter cette vulnérabilité ?

Un attaquant non authentifié pourrait appeler une méthode sur l'interface LSARPC et forcer le contrôleur de domaine à s'authentifier sur un autre serveur avec NTLM. Cette mise à jour de sécurité bloque les appels d'API concernés OpenEncryptedFileRawA et OpenEncryptedFileRawW par le biais de l'interface LSARPC.

Existe-t-il d'autres informations relatives à la protection de mon système ?

Oui. Consultez l'avis ADV210003 - Atténuation des attaques par relais NTLM sur les services de certificats Active Directory (AD CS).

Y a-t-il d'autres mesures à prendre pour protéger le système après l'application de la mise à jour de sécurité ?

Oui. Pour plus d'informations sur les étapes à effectuer pour protéger votre système, consultez l'article KB5005413. Le score CVSS combiné serait de 9.8 si cette vulnérabilité associée à des attaques par relais NTLM sur les services de certificats Active Directory (AD CS).

Dois-je donner la priorité à la mise à jour des contrôleurs de domaine lors de l'application des mises à jour de sécurité publiées le 10 août 2021 ?

Oui. Cette vulnérabilité touche tous les serveurs, mais les contrôleurs de domaine doivent être prioritaires en ce qui concerne l'application des mises à jour de sécurité.

Quel est l'impact de l'installation des mises à jour corrigeant cette CVE sur mon environnement ?

L'API EFS OpenEncryptedFileRaw(A/W), fréquemment utilisée dans les logiciels de sauvegarde, continue à fonctionner dans toutes les versions de Windows (locales et distantes), sauf en cas de sauvegarde sur ou à partir d'un système Windows Server 2008 SP2. OpenEncryptedFileRaw ne fonctionne plus sous Windows Server 2008 SP2.

Remarque : Si vous ne parvenez pas à utiliser un logiciel de sauvegarde sous Windows 7 Service Pack 1 et Windows Server 2008 R2 Service Pack 1 et les versions ultérieures après avoir installé les mises à jour corrigeant cette CVE, contactez le développeur de ce logiciel pour obtenir des mises à jour et un support.

Remerciements

Microsoft reconnaît les efforts des professionnels de la sécurité qui contribuent à protéger les clients par une divulgation coordonnée des vulnérabilités. Pour plus d'informations, consultez la page Remerciements.