サイバー攻撃対策通信
（令和7年第６号）

令和７年７月17日

福岡県警察

Citrix製品の複数の脆弱性について

令和７年６月、Citrix社は同社製品のNetScaler ADC※1及びNetScaler Gateway※2に関する3つの脆弱性情報を公開しました。そのうち「CVE-2025-5777」については既知の悪用された脆弱性（KEV）カタログに追加されました。

同社製品の脆弱性については、CISA※3が令和５年にランサムウェア「*LockBit3.0*」による悪用について報告しています。さらに、警察庁の調査によると、同攻撃は令和５年及び令和６年に国内で最も多く確認されたランサムウェア攻撃です。今回確認された脆弱性も悪用される可能性があり、攻撃のリスクは否定できません。

つきましては、下記バージョンのCitrix社製品をお使いの場合は、修正パッチの早期適用を推奨します。

【公開された脆弱性情報】

※1 **NetScaler ADC**：Webアプリケーションの高速かつ安産な配信を最適化するための製品
※2 **NetScaler Gateway**：リモートアクセスをセキュアに行うためのソリューション
※3 **CISA**：アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁

［6/17公開］

○ CVE-2025-5349：【CVSS v4.0 ベーススコア8.7（重要）】
認証されていない攻撃者が管理機能にアクセスし、ネットワーク内で不正な変更や内部移動を引き起こす可能性があります。

○ CVE-2025-5777：【CVSS v4.0 ベーススコア9.3（緊急）】
NetscalerがGateway又はAAA仮想サーバとして構成されている場合、攻撃者は乗っ取ったセッションを介して、セッショントークや認証情報などのメモリ内情報を読み取る恐れがあります。

［6/25公開］

○ CVE-2025-6543:【CVSS v4.0 ベーススコア9.2（緊急）】
メモリオーバーフローによるサービス拒否、意図しない制御を実現する可能性があります。

【パッチ(修正済ファームウェア:6/27時点)】

CVE-2025-5349及び CVE-2025-5777		CVE-2025-6543	
脆弱なバージョン	パッチ	脆弱なバージョン	パッチ
14.1(14.1-43.56)	14.1-43.56+	14.1(14.1-47.46)	14.1-47.46+
13.1(13.1-58.32)	13.1-58.32+	13.1(13.1-59.19)	13.1-59.19+
13.1-FIPS (13.1-37.235-FIPS未満)	13.1-FIPS 13.1-37.235+	13.1-FIPS (13.1-37.236-FIPS未満)	13.1-FIPS 13.1-37.236+

参考URL① https://www.cisa.gov/news-events/alerts/2025/07/10/cisa-adds-one-known-exploited-vulnerability-catalog
② https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_5349_and_CVE_2025_5777
③ https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_6543

開発者が提供する最新の情報を確認し、対策を早急に検討いただきますよう、よろしくお願いします。

福岡県警察サイバー攻撃対策隊（公安第一課第七係）電話番号：092-641-4141