GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel : (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPP 9108 Port-Vila, Vanuatu
Tél: (678) 33380

1er septembre 2025

Avis 95 : Multiples vulnérabilités affectant les produits NetScaler ADC (anciennement Citrix ADC) et NetScaler Gateway (anciennement Citrix Gateway)
Date de publication : 26 août 2025
Degré d'impact : ÉLEVÉ/CRITIQUE
TLP : CLAIR

CERT Vanuatu (CERTVU) et le service de Communication et de Transformation numérique (SCTN) publient la présente alerte.

Cette alerte s'adresse aux organisations et individus utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de système.

Objet de l'alerte

CERTVU souhaite vous informer des vulnérabilités suivantes affectant les produits NetScaler ADC (anciennement Citrix ADC) et NetScaler Gateway (anciennement Citric Gateway) :

- **CVE-2025-7775 (Critique)** concerne une vulnérabilité de débordement de mémoire pouvant entrainer une exécution de code à distance et/ou un déni de service.
- **CVE-2025-7776 (Élevé)** implique une vulnérabilité de débordement de mémoire entraînant un fonctionnement imprévisible ou erroné et un déni de service.
- **CVE-2025-8424 (Élevé)** concerne un contrôle d'accès inapproprié sur l'interface de gestion NetScaler.

Systèmes concernés

Les versions suivantes de NetScaler ADC et NetScaler Gateway sont affectées.

- NetScaler ADC et NetScaler Gateway 14.1 AVANT 14.1-47.48
- NetScaler ADC et NetScaler Gateway 13.1 AVANT 13.1-59.22
- NetScaler ADC 13.1-FIPS et NDcPP AVANT 13.1-37.24-FIPS et NDcPP
- NetScaler ADC 12.1-FIPS et NDcPP AVANT 12.1-55.330-FIPS et NDcPP

Citrix signale que l'exploitation active de ces vulnérabilités a été observée.

Implication

- **CVE-2025-7775 (Critique)** – Les attaquants peuvent exploiter un débordement de mémoire pré-authentification pour exécuter du code arbitraire sur NetScaler ou le bloquer, ce qui autorise l'accès à distance ou provoque un déni de service (DoS).
- **CVE-2025-7776 (Élevé)** – Les attaquants peuvent exploiter un débordement de mémoire dans les configurations PCoIP Gateway pour provoquer des arrêts de service ou un fonctionnement erratique, perturbant ainsi l'accès au bureau à distance.
- **CVE-2025-8424 (Élevé)** – Les attaquants ayant accès aux interfaces de gestion peuvent contourner les contrôles d'accès et s'emparer des configurations, élargir leurs privilèges ou abuser des ressources administratives.

Mesures d’atténuation

CERTVU conseille à tous les administrateurs de système/réseau et au personnel informatique des organisations de vérifier leurs réseaux afin de détecter toute utilisation d'instances vulnérables des produits NetScaler.

Le **bulletin de sécurité Citrix** doit être consulté pour obtenir des conseils sur la détection et la mise à jour des vulnérabilités de ces produits.

Des informations supplémentaires sont également disponibles dans **la mise à jour de sécurité Citrix annoncée pour NetScaler Gateway et NetScaler.**

Références

1. https://www.cve.org/CVERecord?id=CVE-2025-7775
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938
4. https://www.netscaler.com/blog/news/critical-security-update-announced-for-netscaler-gateway-and-netscaler/