aDvens

Security for the greater good

Bulletin d’alerte
Vulnérabilité critique dans Citrix

2024-01-17 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

Sommaire

Citrix NetScaler - CVE-2023-6549 et CVE-2023-6548

Le 16 janvier 2024, Citrix a publié un bulletin d'alerte concernant deux zéro-day exploitées dans NetScaler ADC (anciennement Citrix ADC) et NetScaler Gateway (anciennement Citrix Gateway).

CVE-2023-6549

Cette faille permet à un attaquant distant et non authentifié de provoquer un déni de service.

Peu d'informations techniques concernant la vulnérabilité ont été publiées, mais Citrix précise que les Netscaler configurés comme passerelle (*VPN virtual server*, *ICA Proxy*, *CVPN*, *RDP Proxy*) ou en *serveur virtuel AAA* sont vulnérables.

Cette vulnérabilité est activement exploitée.

Type de vulnérabilité

- CWE-119 : Improper Restriction of Operations within the Bounds of a Memory Buffer

Risque

- Déni de service

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Aucun
Privilèges requis	Aucun	Impact sur l'intégrité	Faible
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

CVE-2023-6548

Cette faille permet à un attaquant, ayant un accès à l'interface de gestion de NetScaler, d'exécuter du code arbitraire sur celui-ci.

Cette vulnérabilité est activement exploitée.

Type de vulnérabilité

- CWE-94 : Improper Control of Generation of Code ('Code Injection')

Risque

- Exécution de code arbitraire

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Adjacent	Portée	Inchangée
Complexité d'attaque	Faible	Impact sur la confidentialité	Faible
Privilèges requis	Faible	Impact sur l'intégrité	Faible
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Faible

Produits impactés

NetScaler ADC (ancienement Citrix ADC) :

- Versions 12.1 et antérieures
- Versions 12.1-NDcPP antérieures à 12.1-55.302
- Versions 12.1-FIPS antérieures à 12.1-55.302
- Versions 13.0 antérieures à 13.0-92.21
- Versions 13.1-FIPS antérieures à 13.1-37.176
- Versions 13.1 antérieures à 13.1-51.15
- Versions 14.1 antérieures à 14.1-12.35

NetScaler Gateway (ancienement Citrix Gateway) :

- Versions 12.1 et antérieures
- Versions 13.0 antérieures à 13.0-92.21
- Versions 13.1 antérieures à 13.1-51.15
- Versions 14.1 antérieures à 14.1-12.35

Recommandations

- Mettre à jour NetScaler ADC vers la version 12.1-55.302, 13.0-92.21, 13.1-37.176, 13.1-51.15, 14.1-12.35 ou ultérieure.
- Mettre à jour NetScaler Gateway vers la version 13.0-92.21, 13.1-51.15, 14.1-12.35 ou ultérieure.
- Des informations complémentaires sont disponibles dans le bulletin de Citrix.

Preuve de concept

Aucune preuve de concept n'est disponible en source ouverte.

Références

- https://www.cve.org/CVERecord?id=CVE-2023-6548
- https://www.cve.org/CVERecord?id=CVE-2023-6549
- https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549
- https://www.bleepingcomputer.com/news/security/citrix-warns-of-new-netscaler-zero-days-exploited-in-attacks/