aDvens

Security for the greater good

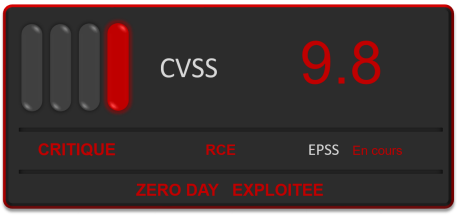
Newscast

Vulnérabilité critique CITRIX

2022-12-14 | **TLP:CLEAR** | CERT aDvens - CTI
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

1. CVE-2022-27518 (Critique)



La société CITRIX publie le 13 décembre, un bulletin de sécurité alertant sur une vulnérabilité affectant ses produits ***Citrix ADC*** et ***Citrix Gateway***, configurés en mode *SAML SP* et *SAML IdP*.

Un défaut de contrôle des ressources permet à un attaquant distant et non authentifié, d'exécuter du code arbitraire sur le système.

Cette vulnérabilité est exploitée.

1.1. Risque

- Exécution de code arbitraire à distance.

1.2. Type de vulnérabilité

- **CWE-664**: Improper Control of a Resource Through its Lifetime.

1.3. Criticité

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

1.4. Produits impactés

Citrix ADC et Gateway 13.0

- Dans leurs versions antérieures à 13.0-58.32.

Citrix ADC et Gateway 12.1

- Dans leurs versions antérieures à 12.1-65.25.

Citrix ADC 12.1-FIPS

- Dans leurs versions antérieures à 12.1-55.291.

Citrix ADC 12.1-NDcPP

- Dans leurs versions antérieures à 12.1-55.291.

Pour déterminer si un produit Citrix ADC ou Gateway est configuré comme **SAML SP** ou **SAML IdP**, les instructions suivantes sont renseignées dans le fichier de configuration *ns.conf*.

configuration SAML SP

```
add authentication samlAction
```

configuration SAML IdP

```
add authentication samlIdPProfile
```

1.5. Recommandations

- Mettre à jour Citrix ADC et Citrix Gateway vers les versions 13.0-58.32 et suivantes.
- Mettre à jour Citrix ADC et Citrix Gateway vers la version 12.1-65.25 et versions suivantes de 12.1.
- Mettre à jour Citrix ADC 12.1-FIPS vers la version 12.1-55.291 et versions suivantes de 12.1-FIPS.
- Mettre à jour Citrix ADC 12.1-NDcPP vers la version 12.1-55.291 et versions suivantes de 12.1-NDcPP.

Les versions antérieures à 12.1 de Citrix ADC et Gateway ne sont plus maintenues par l'éditeur. Ce dernier recommande de mettre à jour vers une version plus récente.

1.6. Exploitation de la vulnérabilité

L'agence nationale de sécurité américaine *NSA*, alerte dans son bulletin du 13 décembre, sur l'exploitation de la vulnérabilité par le groupe cybercriminel chinois **APT-5**. La NSA met à disposition des règles **YARA** pour détecter un implant malveillant utilisé par l'attaquant.

```
rule tricklancer_a {
strings:
$str1 = "//var//log//ns.log" nocase ascii wide
$str2 = "//var//log//cron" nocase ascii wide
$str3 = "//var//log//auth.log" nocase ascii wide
$str4 = "//var//log//httpaccess-vpn.log" nocase ascii wide
$str5 = "//var//log//nsvpn.log" nocase ascii wide
$str6 = "TF:YYYYMMddhhmmss" nocase ascii wide
$str7 = "//var//log//lastlog" nocase ascii wide
$str8 = "clear_utmp" nocase ascii wide
$str9 = "clear_text_http" nocase ascii wide
condition:
7 of ($str*)}
rule tricklancer_b {
strings:
$str1 = "nsppe" nocase ascii wide
$str2 = "pb_policy -h nothing" nocase ascii wide
$str3 = "pb_policy -d" nocase ascii wide
$str4 = "findProcessListByName" nocase ascii wide
$str5 = "restoreStateAndDetach" nocase ascii wide
$str6 = "checktargetsig" nocase ascii wide
$str7 = "DoInject" nocase ascii wide
$str8 = "DoUnInject" nocase ascii wide
condition:
7 of ($str*)
}
```

```
rule tricklancer_c {
strings:
$str1 = "is_path_traversal_or_vpns_attack_request" nocase ascii wide
$str2 = "ns_vpn_process_unauthenticated_request" nocase ascii wide
$str3 = "mmapshell" nocase ascii wide
$str4 = "DoUnInject" nocase ascii wide
$str5 = "CalcDistanse" nocase ascii wide
$str6 = "checkMyData" nocase ascii wide
$str7 = "vpn_location_url_len" nocase ascii wide
condition:
5 of ($str*)
}
```

1.7. Preuve de concept

Actuellement, aucune preuve de concept (POC) n'est disponible en sources ouvertes.

2. Références

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27518
- https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518
- https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/
- https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF