RCE CVE-2023-3519 - Citrix ADC and Citrix Gateway

Luglio 2023

Report Informativo SOC

Dettagli documento

Titolo attività
RCE CVE-2023-3519 - Citrix ADC and Citrix Gateway

Sintesi attività
Report contenente le evidenze relative alla vulnerabilità critica CVE-2023-3519 che colpisce i prodotti Citrix ADC e Citrix Gateway

Destinatario pubblicazione
Referenti servizi SOC e SOC AdS

Livello di riservatezza (Clear/Green/Amber/Amber+Strict/Red)
CLEAR

Data pubblicazione
24/07/2023

Redatto da
Mirko Ioris

Revisionato da
Massimo Giaimo

Riservatezza della pubblicazione

Al documento viene applicato un livello di riservatezza, avvalorato dalla voce “Livello di riservatezza” presente in prima pagina. I valori utilizzabili (RED / AMBER / GREEN / CLEAR) hanno i seguenti significati:

TLP:RED = Riservato ai soli partecipanti.

> Le fonti possono utilizzare TLP:RED quando le informazioni non possono essere efficacemente utilizzate da altre parti e potrebbero avere un impatto sulla privacy, sulla reputazione o sulle operazioni di una parte se utilizzate in modo improprio. I destinatari non possono condividere le informazioni TLP:RED con parti al di fuori dello specifico scambio, riunione o conversazione in cui sono state originariamente divulgate. Nel contesto di una riunione, ad esempio, le informazioni di TLP:RED sono limitate ai presenti alla riunione. Nella maggior parte dei casi, TLP:RED dovrebbe essere scambiato verbalmente o di persona.

TLP:AMBER = Divulgazione limitata, riservata alle organizzazioni dei partecipanti.

TLP:AMBER+STRICT limita la condivisione solo all'*organizzazione*.

> Le fonti possono utilizzare TLP:AMBER quando le informazioni richiedono supporto per agire in modo efficace, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise al di fuori delle organizzazioni coinvolte. I destinatari possono condividere le informazioni TLP:AMBER solo con i membri della propria organizzazione e con clienti o clienti che hanno bisogno di conoscere le informazioni per proteggersi o prevenire ulteriori danni.
>
> Nota: se la fonte desidera limitare la condivisione **solo** all'organizzazione, deve specificare TLP:AMBER+STRICT.

TLP:GREEN = Divulgazione limitata, riservata alla comunità.

> Le fonti possono utilizzare TLP:GREEN quando le informazioni sono utili per la consapevolezza di tutte le organizzazioni partecipanti, nonché con i colleghi all'interno della comunità o del settore più ampio. I destinatari possono condividere le informazioni TLP:GREEN con colleghi e organizzazioni partner all'interno del loro settore o comunità, ma non tramite canali pubblicamente accessibili. Le informazioni in questa categoria possono essere ampiamente diffuse all'interno di una particolare comunità. Le informazioni TLP:GREEN potrebbero non essere rilasciate al di fuori della community.

TLP:CLEAR = La divulgazione non è limitata.

Le fonti possono utilizzare TLP:CLEAR quando le informazioni comportano un rischio minimo o prevedibile di uso improprio, in conformità con le regole e le procedure applicabili per il rilascio pubblico. Fatte salve le norme standard sul copyright, le informazioni TLP:CLEAR possono essere distribuite senza restrizioni.

Indice

Introduzione

Citrix Systems, un'azienda statunitense di cloud computing che fornisce tecnologie per la virtualizzazione in tutto il mondo, ha pubblicato il giorno 18 luglio 2023 un bollettino di sicurezza riguardante **tre** vulnerabilità presenti sui due dei loro prodotti: **Citrix ADC** e **Citrix Gateway** [1].

CVE ID	Affected Products	Description	Pre-requisites	CWE	CVSS
CVE-2023-3466	Citrix ADC, Citrix Gateway	Reflected Cross-Site Scripting (XSS)	Requires victim to access an attacker-controlled link in the browser while being on a network with connectivity to the NSIP	ⓘ CWE-20	8,3
CVE-2023-3467	Citrix ADC, Citrix Gateway	Privilege Escalation to root administrator (nsroot)	Authenticated access to NSIP or SNIP with management interface access	ⓘ CWE-269	8
CVE-2023-3519	Citrix ADC, Citrix Gateway	Unauthenticated remote code execution	Appliance must be configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) OR AAA virtual server	ⓘ CWE-94	9,8

Il dettaglio delle vulnerabilità sul sito di Citrix

La vulnerabilità CVE-2023-3519, classificata come **critica**, ha ricevuto una particolare attenzione mediatica dalla community di esperti in cyber security, essendo stata già sfruttata da criminali in azioni di attacco ed essendo presenti migliaia di dispositivi ancora vulnerabili esposti online.

Panoramica sull'attacco

La vulnerabilità critica **CVE-2023-3519** è apparsa online la prima volta verso l'inizio di luglio, quando un threat actor ha iniziato a pubblicizzarla come falla zero-day su un forum di hacker. Non appena Citrix ha saputo della notizia ha iniziato a lavorare su una patch, rilasciando il 18 luglio insieme alle correzioni di altre due vulnerabilità classificate con criticità alta.

- CVE-2023-3466 - Reflected Cross-Site Scripting (XSS) [2]
- CVE-2023-3467 - Privilege Escalation to root administrator (nsroot) [3]
- CVE-2023-3519 - Unauthenticated remote code execution [4]

Il giorno seguente, 19 luglio, la CISA (Cybersecurity & Infrastructure Security Agency) ha aggiunto la vulnerabilità al suo catalogo KEV (Known Exploited Vulnerabilities), descrivendola come una vulnerabilità di code injection che consente l'esecuzione di codice remoto non autenticato.

I criminali stanno sfruttando questa falla per rilasciare una webshell sugli applicativi NetScaler ADC vulnerabili al fine di **collezionare** ed **esfiltrare** dati contenuti nell'**active directory** (AD) della vittima.

Le versioni vulnerabili sono riportate di seguito, si raccomanda di aggiornare ad una versione successiva il più presto possibile:

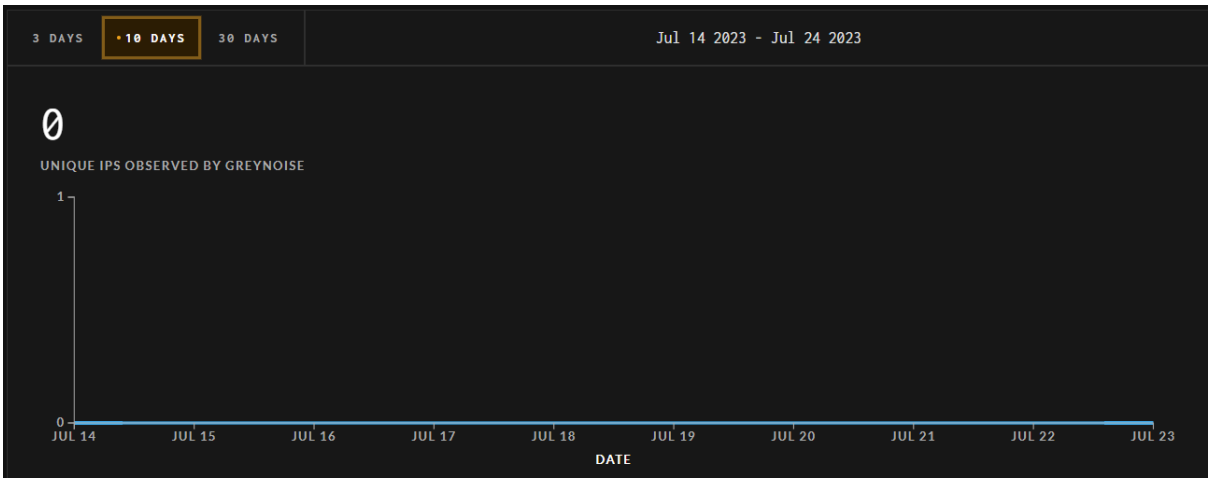
- NetScaler ADC e NetScaler Gateway 13.1 prima dell'update 13.1-49.13
- NetScaler ADC e NetScaler Gateway 13.0 prima dell'update 13.0-91.13
- NetScaler ADC 13.1-FIPS prima dell'update 13.1-37.159
- NetScaler ADC 12.1-FIPS prima dell'update 12.1-55.297
- NetScaler ADC 12.1-NDcPP prima dell'update 12.1-55.297

Analisi della vulnerabilità

Vari ricercatori hanno analizzato le differenze tra la nuova versione patchata e la precedente vulnerabile per comprendere meglio di cosa si trattasse la vulnerabilità identificata. **Rapid7** [5] e **Assetnote** [6] hanno riportato analisi molto dettagliate concludendo che il problema sembra riguardare i componenti di elaborazione SAML di Citrix ADC e Citrix Gateway. Nella versione non patchata non c'è un controllo dei limiti ed è possibile scrivere fuori dalla fine dell'array. Questo overflow dell'heap durante l'analisi di alcuni tipi di richieste SAML corrompe il resto della struttura e qualsiasi memoria allocata successiva.

Ulteriori ricerche però, come quella condotta da **Bishopfox** [7], hanno individuato una vulnerabilità che non richiede l'abilitazione di SAML ma solo che il dispositivo sia configurato come gateway o server virtuale AAA e che esponga un percorso vulnerabile specifico che sembra essere abilitato per impostazione predefinita in alcune installazioni.

Data la mancanza di requisiti SAML, si ritiene che quest'ultima vulnerabilità di stack overflow sia quella menzionata e riconosciuta come CVE-2023-3519, e che il bug del parser SAML sia una vulnerabilità separata che è stata patchata senza un advisory associato. Bishopfox non si è fermata qui e ha collaborato con **GreyNose** [8] nella creazione di un tag per identificare eventuali IP che provano ad autenticarsi a piattaforme vulnerabili Citrix ADC & Gateway utilizzando la CVE-2023-3519.



Negli ultimi 10 giorni non ci sono evidenze di IP che hanno tentato di exploitare la vulnerabilità

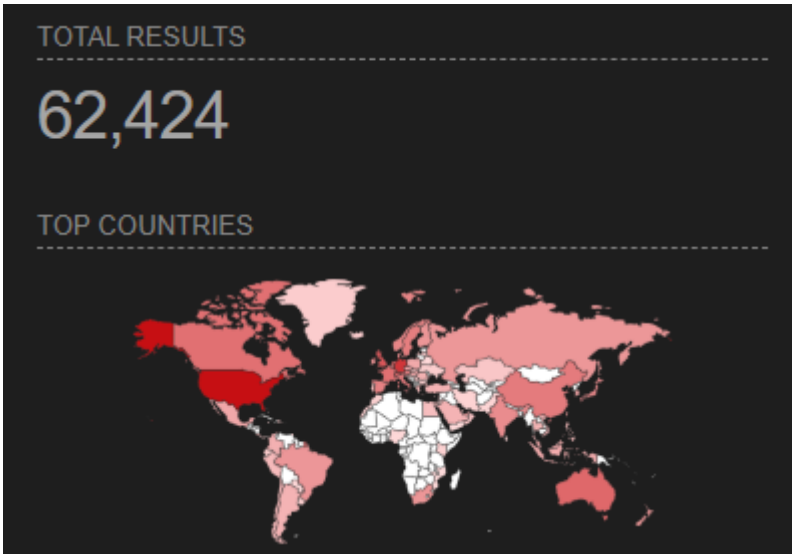
Superficie d'attacco

Utilizzando motori di ricerca dedicati ai dispositivi, come **Shodan**, è possibile fare delle query per visualizzare il numero di macchine Citrix ADC e Gateway pubblicamente raggiungibili. Una possibilità è quella di cercare per **favicon**. Le favicon sono le immagini che vengono mostrate nella scheda del browser della pagina visitata. Alcuni esempi:

Le favicon del NetEye blog e di Google

Di seguito sono riportati i dispositivi trovati con le query Shodan (data ricerca 24/07/2023):

Query per favicon
http.favicon.hash:-1292923998,-1166125415



Per comprendere quanti di questi 60mila dispositivi sono vulnerabili possiamo utilizzare uno degli script messi a disposizione dalla community. Sono infatti stati sviluppati numerosi scanner per identificare la presenza della CVE-2023-3519, eccone alcuni:

- https://github.com/telekom-security/cve-2023-3519-citrix-scanner
- https://github.com/securekomodo/citrixInspector
- https://github.com/RootUp/PersonalStuff/blob/master/http-vuln-cve2023-3519.nse
- https://github.com/mr-r3b00t/CVE-2023-3519/tree/main
- https://github.com/assetnote/exploits/tree/main/citrix/CVE-2023-3519

Abbiamo testato i primi 1000 risultati e questo è quello che abbiamo trovato:

Stato	**Nr. di indirizzi IP**
Patchato	532
Potenzialmente vulnerabile	270
Non verificabile	198

Come possiamo notare poco più della metà sono stati patchati, mentre quasi un terzo sono ancora potenzialmente vulnerabili nonostante sia passata quasi una settimana dal rilascio della patch. Se riportiamo questo risultato sui 60k dispositivi inizialmente trovati il numero delle istanze potenzialmente vulnerabili aumenta considerevolmente.

Fortunatamente non sono stati registrati molti attacchi che sfruttano la vulnerabilità, al momento solo i seguenti IOC sono stati segnalati [9]:

- 216[.]41[.]162[.]172
- 216[.]51[.]171[.]17

Raccomandiamo in ogni caso di aggiornare i dispositivi alle versioni non più vulnerabili qualora ne faceste uso.

Come proteggersi

Citrix ha già pubblicato le patch che risolvono le vulnerabilità citate in questo report, pertanto raccomandiamo di aggiornare i propri dispositivi alle seguenti versioni:

- NetScaler ADC e NetScaler Gateway 13.1-49.13 e versioni successive
- NetScaler ADC e NetScaler Gateway 13.0-91.13 e versioni successive di 13.0
- NetScaler ADC 13.1-FIPS 13.1-37.159 e versioni successive di 13.1-FIPS
- NetScaler ADC 12.1-FIPS 12.1-55.297 e versioni successive di 12.1-FIPS
- NetScaler ADC 12.1-NDcPP 12.1-55.297 e versioni successive di 12.1-NDcPP

La versione 12.1 di NetScaler ADC e NetScaler Gateway è in End Of Life (EOL). e viene consigliato ai clienti di aggiornare le proprie appliance a una delle versioni supportate sopra elencate.

Cosa fare nel caso di attacco subito

Ecco la lista di raccomandazioni e contromisure da adottare nel caso un sistema sia stato corrotto [10] :

- Rimuovere l'istanza di NetScaler dalla rete.
- Cambiare la password di tutti gli account LDAP o altri account AD e/o di rete memorizzati sul NetScaler.
- Sostituire i certificati SSL sull'istanza compromessa il prima possibile (le chiavi sono memorizzate in file sul NetScaler e potrebbero essere state lette da un utente malintenzionato).
- Revocare i certificati SSL e le chiavi SSL compromessi.
- Se la macchina colpita è un'appliance VPX e sono presenti snapshot più vecchi di 3 mesi può valere la pena provare a ripristinarli
    - Per sicurezza, esportare il file di configurazione del sistema interessato e copiarlo/ripristinarlo su una nuova appliance VPX.
    - Assicurarsi che venga utilizzato lo stesso indirizzo hardware, altrimenti la licenza non sarà valida e dovrà essere richiesta/importata di nuovo.
    - Disconnettere la rete prima dell'avvio
    - Avviare l'appliance e verificare tramite console che il VPX non sia compromesso

- Cambiare la password nsroot
- Connettere prima solo la rete interna
- Connettere la rete esterna
- Tenere sotto controllo i log

Bibliografia

[1]https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467

[2]https://nvd.nist.gov/vuln/detail/CVE-2023-3466

[3]https://nvd.nist.gov/vuln/detail/CVE-2023-3467

[4]https://nvd.nist.gov/vuln/detail/CVE-2023-3519

[5]https://blog.assetnote.io/2023/07/21/citrix-CVE-2023-3519-analysis/

[6]https://attackerkb.com/topics/si09VNJhHh/cve-2023-3519

[7]https://bishopfox.com/blog/citrix-adc-gateway-rce-cve-2023-3519

[8]https://viz.greynoise.io/tag/citrix-adc-netscaler-cve-2023-3519-rce-attempt

[9]https://socradar.io/critical-and-high-vulnerabilities-in-citrix-adc-and-citrix-gateway-cve-2023-3519-cve-2023-3466-cve-2023-3467/

[10]https://www.deyda.net/index.php/en/2023/07/19/checklist-for-citrix-adc-cve-2023-3519/