TLP: WHITE
Szabadon terjeszthető!

Tájékoztatás

Citrix szerver sérülékenységéről

(2020. január 27.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki a Citrix szervereket érintő, **CVE-2019-19781** számon nyilvántartott **kritikus** kockázati besorolású végpont sérülékenységgel kapcsolatban, amely kihasználásával jogosultságokkal nem rendelkező távoli támadó tetszőleges parancsokat futtathat az érintett szerveren.

A **FireEye** és a **Citrix Systems** együtt létrehoztak egy alkalmazást, amely segít felderíteni, hogy az adott Citrix szerver kompromittálódott-e a fent említett sérülékenység kihasználásának következtében.

A szoftver átvizsgálja a szervert, és az előre megadott **IoC**-k meglétének függvényében az alább felsorolt három kategória egyikébe besorolja azokat.

- Bizonyíték az eszköz kompromittálódásra (Evidence of compromise).
- Bizonyíték, hogy az eszközön sérülékenység vizsgálatot hajtottak végre (Evidence of successful vulnerability scanning).
- Bizonyíték, hogy az eszközön sikertelen sérülékenység vizsgálatot hajtottak végre (Evidence of unsuccessful vulnerability scanning).

A program az alábbi Citrix Application Delivery Controller (ADC), Citrix Gateway, and Citrix SD-WAN WANOP eszközökkel kompatibilis:

- Citrix ADC and Citrix Gateway version 13.0
- Citrix ADC and Citrix Gateway version 12.1
- Citrix ADC and Citrix Gateway version 12.0
- Citrix ADC and Citrix Gateway version 11.1
- Citrix ADC and Citrix Gateway version 10.5
- Citrix SD-WAN WANOP version 10.2.6
- Citrix SD-WAN WANOP version 11.0.3

Intézetünk javasolja a **Citrix Systems Inc** által - a sérülékenységgel kapcsolatban - kiadott két frissítés telepítését, valamint a sérülékenység felderítésére készített szoftver használatát.

Hivatkozások:

Citrix szerver frissítés: https://www.citrix.com/blogs/2020/01/19/vulnerability-update-first-permanent-fixes-available-timeline-accelerated/

Sérülékenység mérséklés: https://support.citrix.com/article/CTX267679

IoC szkenner szoftver: https://github.com/fireeye/ioc-scanner-CVE-2019-19781/

Sérülékenység leírás: https://nki.gov.hu/figyelmeztetesek/serulekenysegek-uj/citrix-adc-es-citrix-gateway-web-szerver-serulekenyseg/

Sérülékenység leírás: https://nvd.nist.gov/vuln/detail/CVE-2019-19781/

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: csirt@nki.gov.hu