Citrix Vulnerability Scanner (CVE-2019-19781) Report

✔ 194.20.61.27

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	0
Low:	0
Info:	0

Scan information:

Start time:	2020-01-13 12:44:35 UTC+02
Finish time:	2020-01-13 12:44:36 UTC+02
Scan duration:	1 sec
Tests performed:	1/1
Scan status:	Finished

Findings

Remode Code Execution in Citrix ADC (CVE-2019-19781) (port 80)

While probing for this vulnerability, the following file was retrieved from remote Citrix server:
https://194.20.61.27:443/vpn/../vpns/cfg/smb.conf

```
[global]

 encrypt passwords = yes

 name resolve order = lmhosts wins host bcast
```

Details

Risk description:
The target Citrix ADC server (also known as NetScaler ADC, Citrix Gateway or NetScaler Gateway) is affected by a Remote Code Execution vulnerability (CVE-2019-19781).
While the root cause of the vulnerability is a path traversal issue, it can be leveraged to arbitrary code execution.
More details about this vulnerability: https://www.mdsec.co.uk/2020/01/deep-dive-to-citrix-adc-remote-code-execution-cve-2019-19781/

Here is a public exploit which allows an attacker to gain a shell on the vulnerable Citrix server: https://www.exploit-db.com/exploits/47902

Recommendation:
We recommend you to follow the mitigation steps proposed by the vendor in order to avoid the risk of this vulnerability:
https://support.citrix.com/article/CTX267679

Scan coverage information

List of tests performed (1/1)

- ✔ Scanning for Citrix CVE-2019-19781 vulnerability...

Scan parameters

Target:	194.20.61.27
Port:	443