Remediation Checklist for CVE-2019-19781

DJ Eshelman

CTXPro.com

There has been a ton of information out there about this historic Citrix NetScaler/ADC flaw - rightfully so as it more or less affects every single one out there. I wanted to create this checklist for you to make sure you've got all of your bases covered. This is the list I'm using with all of my clients that were affected.

If there is anything on this list you don't feel confident about doing, I highly suggest you reach out to myself or someone else in the Citrix community for help!

- DJ Eshelman

□ **Applied the initial mitigation steps listed at https://support.citrix.com/article/CTX267679 to prevent the attack before December 20th, 2019** *(if not... apply it and keep going)*

□ **Checked to validate the mitigation steps using the tool at https://support.citrix.com/article/CTX269180**

□ **Scanned for breaches or access using the Citrix/FireEye tool using at least version 1.2 of the scanning script at** https://github.com/citrix/ioc-scanner-CVE-2019-19781/releases

□ **Documented any noted access and sent to management informing them of the event and action steps taken or being taken**

□ **Save the Configuration and restore the config either a clean upgraded build (firmware) or upgraded restored backup (VPX) from before December 17, 2019. (Note - SDX requires a complete firmware reset, not just a configuration reset)**

□ **Changed the password for any ADC Local accounts**

□ **Changed the passwords or keyphrases for LDAP account, RADIUS or any other accounts noted in the configuration - assured that my LDAP account does not have access to the network beyond ”Domain Users”.**

□ **Directed all Citrix users who have accessed the Citrix Gateway since December to change their passwords**

□ **Re-Keyed SSL Certificates**

DJ Eshelman

CTXPro.com

Need Help?

The tasks required to properly remediate this issue aren't in the normal skillset. But that shouldn't keep you from FULLY remediating this issue. This is a very dangerous flaw of which no step should be ignored.

If you need help learning the steps required, we are thinking of pulling together an online class to do just that - just let us know you're interested.

Consulting Services are also available by many members of our staff and community - reach out to Support@CTXPro.com to get some help... either way we invite you to join us in our very own Mighty Network app on the web or your phone!

Join Our Free Citrix Hero Community