



Home

Support ▾

Downloads ▾

Documentation ▾

Community

Log in

Mitigation Steps for CVE-2019-19781

Title

Mitigation Steps for CVE-2019-19781

CTX Number

CTX267679

Article Type

Problem Solution

Created Date

17/Dec/2019

Last Modified Date

1/Sep/2021

Symptoms or Error

On December 17 2019 Citrix released security bulletin [CTX267027](#): A vulnerability in Citrix Application Delivery Controller (ADC), formerly known as NetScaler ADC, and Citrix Gateway, formerly known as NetScaler Gateway, that could lead to arbitrary code execution.

Further investigation by Citrix has shown that this issue also affects certain deployments of Citrix SDWAN, specifically Citrix SDWAN WANOP edition. Citrix SDWAN WANOP edition packages Citrix ADC as a load balancer thus resulting in the affected status.

Solution

The following configuration changes on Citrix ADC and Citrix Gateway serve as a mitigation to the aforementioned vulnerability.

To mitigate the vulnerability on relevant WANOP devices, the same steps will need to be applied to the Citrix ADC load balancer instance residing on the WANOP device. The Citrix ADC instance and associated details are listed on the WANOP GUI under Configuration (Overview) > Maintenance > Instances > Load Balancer. The credentials for this ADC instance are assigned by the administrator during deployment. The administrator will need to login to the ADC instance using these credentials to apply the mitigations. The following Standalone System instructions are applicable to the Citrix ADC on the WANOP device as well.

As always, please ensure that the system configuration has been saved in its current state before embarking on the mitigations. The procedure involves rebooting instances and may cause temporary data to be lost in the process.

Standalone System

Run the following commands from the command line interface of the ADC or Gateway appliance to create a responder action and policy:

```
enable ns feature responder
add responder action respondwith403 respondwith "\"HTTP/1.1 403 Forbidden\r\n\r\n\""
add responder policy ctx267027 "HTTP.REQ.URL.DECODE_USING_TEXT_MODE.CONTAINS(\"/vpns/\") && (!CLIENT.SSLVPN.IS_SSLVPN || HTTP.REQ.URL.DECOD
bind responder global ctx267027 1 END -type REQ_OVERRIDE
save config
```

The following section is to ensure that the changes apply to the management interfaces as well. From the command line interface, please run the following commands:

```
shell nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0
shell "echo 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' >> /nsconfig/rc.netscaler"
reboot
```

HA Pair

On primary:



```
enable ns feature responder
add responder action respondwith403 respondwith "\"HTTP/1.1 403 Forbidden\r\n\r\n\""
add responder policy ctx267027 "HTTP.REQ.URL.DECODE_USING_TEXT_MODE.CONTAINS(\"/vpns/\") && (!CLIENT.SSLVPN.IS_SSLVPN || HTTP.REQ.URL.DECOD
bind responder global ctx267027 1 END -type REQ_OVERRIDE
save config
shell nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0
shell "echo 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' >> /nsconfig/rc.netscaler"
reboot
```

On secondary (after primary comes up):

```
shell nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0
shell "echo 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' >> /nsconfig/rc.netscaler"
reboot
```

Please ensure that the secondary node has the 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' command present in the file - /nsconfig/rc.netscaler.

The reboot process will retain the current primary as the primary even after the reboot. However, the customer is free to follow the reboot order used in the standard HA pair upgrade.

Cluster

On CLIP:

```
enable ns feature responder
add responder action respondwith403 respondwith "\"HTTP/1.1 403 Forbidden\r\n\r\n\""
add responder policy ctx267027 "HTTP.REQ.URL.DECODE_USING_TEXT_MODE.CONTAINS(\"/vpns/\") && (!CLIENT.SSLVPN.IS_SSLVPN || HTTP.REQ.URL.DECOD
bind responder global ctx267027 1 END -type REQ_OVERRIDE
save config
shell nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0
shell "echo 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' >> /nsconfig/rc.netscaler"
shell reboot
```

On each cluster node:

```
shell nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0
shell "echo 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' >> /nsconfig/rc.netscaler"
shell reboot
```

Please ensure that all cluster nodes have the 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' command present in their respective /nsconfig/rc.netscaler files.

If the cluster has to be up during the mitigation procedure, please ensure that the node that gets rebooted re-joins the cluster (i.e., the operational state turns from Unknown to Active) before rebooting other nodes in the cluster.

Admin partition

```
switch ns partition <partition_name>
enable ns feature responder
add responder action respondwith403 respondwith "\"HTTP/1.1 403 Forbidden\r\n\r\n\""
add responder policy ctx267027 "HTTP.REQ.URL.DECODE_USING_TEXT_MODE.CONTAINS(\"/vpns/\") && (!CLIENT.SSLVPN.IS_SSLVPN || HTTP.REQ.URL.DECOD
bind responder global ctx267027 1 END -type REQ_OVERRIDE
save config
```

To emphasize, please be sure to apply the above steps on all the individual partitions, including default. Then run the following steps on the default partition.

```
switch ns partition default
shell nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0
shell "echo 'nsapimgr_wr.sh -ys skip_systemaccess_policyeval=0' >> /nsconfig/rc.netscaler"
reboot
```



Procedure to revert the changes



These steps are applicable to the Standalone System, CLIP on Cluster, and HA Primary in a HA Pair, and to each Admin Partition. This series of steps may also be carried out upon upgrading to the fixed builds once available.

```
unbind responder global ctx267027
rm responder policy ctx267027
rm responder action respondwith403
save config
```

The command below is designed to search within a file for the specified pattern, and consequently remove the line that was originally added. This will effectively remove the nsapimgr command from the file - rc.netscaler.

```
shell nsapimgr_wr.sh -ys skip_systemaccess_policyeval=1
shell "sed -i '' '/skip_systemaccess_policyeval=0/d' /nsconfig/rc.netscaler"
reboot
```

The reboot, in each of the scenarios above, is not necessary to apply the policy, but is rather a precautionary and recommended step to ensure that open sessions obtained via the vulnerability prior to policy application, if any, are cleared.

Additional Information

Priority conflict

The priority given to the responder policy is 1. If there are any other responder policies bound with the same priority, the policy binding might fail. Customers are advised to adjust the priorities of other policies appropriately while making sure that the policy recommended in this article receives priority '1'.

The ‘skip_systemaccess_policyeval’ Flag

This flag ensures that the responder policies are evaluated on the admin portal traffic.

If the admin portal IP is in a secured environment, this flag is not needed.

Enabling this might cause some obstruction to some admin pages. In such a case, the customer can toggle the flag during their maintenance window and set it back to the value ‘1’.

Nodes that are removed from a cluster are vulnerable

When a cluster node is removed, its configuration is cleared. As such, the responder policies listed above and hence the protection that comes with them are also cleared. The node would consequently lose the protections provided by these mitigation steps.

Plugin download link from Admin UI

The current admin UI has a link to download the plugins (/vpns/scripts/vista/*.exe). This link contains "/vpns/" in its path and thus will not be accessible after this fix.

/vpns/ in a legitimate URL

If there is any backend webserver resource which has /vpns/ in its path, that resource will be blocked.

Additional Resources

- CTX269190- [Issues with accessing Gateway, launching apps/desktops, authentication after applying CVE-2019-19781 mitigation steps](#)
- CTX269189 - [Vulnerability still exists after mitigation steps for CVE-2019-19781 applied](#)
- CTX269188- [Cannot download Gateway VPN plug-in after applying CVE-2019-19781 mitigation steps](#)


NetScaler

Netscaler Gateway

Citrix SD-WAN WANOP

Was this article helpful? ★ ★ ★ ★ ★



 Site feedback

FOLLOW CITRIX   



[Legal](#) | [Do Not Sell My Personal Information](#) | [Cookie Preferences](#)

© 2024 Cloud Software Group, Inc. All rights reserved.

