THREAT BULLETINS

APT5: Citrix Application Delivery Controller (ADC) Threat Hunting Guidance

TLP:WHITE

Dec 13, 2022

On December 13, 2022, the National Security Agency (NSA) released a Cybersecurity Advisory (CSA) to provide threat hunting guidance for Citrix Application Delivery Controller (ADC) deployments. APT5, also known as UNC2630 and MANGANESE, is a Chinese state-sponsored group that has demonstrated targeting capabilities against environments with Citrix ADC deployments leading to illegitimate access to targeted organizations via the bypass of normal authentication controls.

NSA recommends organizations hosting Citrix ADC environments take the steps provided as part of their investigation. The detection mechanisms should be treated as independent ways of identifying potentially malicious activity on impacted systems. Findings may vary based on the environment and the stage of the detected activity. As such, NSA recommends investigating any positive result even if other detections return no findings.

Please note that this guidance does not represent all techniques, tactics, or procedures (TTPs) the actors may use when targeting Citrix ADC environments.

All members are encouraged to review APT5: Citrix ADC Threat Hunting Guidance for guidance on file integrity and behavioral checks, provided detections, and mitigations.

Citrix has provided information advising which Citrix ADC and Citrix Gateway versions are affected by CVE-2022-27518 in addition to recommended next steps on their blog, available here.

File Integrity:
A malicious actor enabling continued access will likely require modification to legitimate binaries. Therefore, NSA recommends organizations regularly check key executables in their environments for any deviations from the known good copies associated with their running version. Key executables are those binaries essential for proper execution of the Citrix ADC appliance. These files include, but may not be limited to: nsppe, nsaaad, nsconf, nsreadfile, and nsconmsg. The following command can be executed from a shell to facilitate this comparison:

cd /netscaler ; for i in "nsppe nsaaad nsconf nsreadfile nsconmsg"; do md5 ${i} ; done

The MD5 hashes should be compared to known good hashes from the vendor or hashes of the respective binaries from a known good copy downloaded from the vendor. Any deviation requires further investigation.

Additionally, the following command can indicate tampering by one APT5 technique. This is indicated by one line of output, but no output otherwise:

procstat –v $(pgrep –o –i nsppe) | grep "0x10400000 " | grep "rwx"

NSA also recommends that organizations take scheduled tech support bundles1 and/or snapshots of their running environment and store them in an offline or otherwise immutable location to create a forensic history of systems. These backups can be used to compare running instances or to reconstruct events if suspicious activity is identified.

Behavioral Checks:
In addition to any alterations of legitimate binaries, some of APT5's activities may be visible in various system logs. NSA recommends that organizations leverage off-device logging mechanisms for all system logs, to include dmesg and ns.log, and actively monitor them for the following activity:

- Instances of pb_policy appearing in logs without being linked to expected administrator activity.

- The actors have been seen leveraging tools that run 'pb_policy' twice. This creates the following logs in ns.log:

<local0.info> [hostname] pb_policy: Changing pitboss policy from X to Y
<local0.info> [hostname] pb_policy: Changing pitboss policy from Y to X

  - Where X and Y are constant values for your system.
  - Gaps in logs, or mismatches between logs on the device and in your remote logging solution.
  - Legitimate user account activity without a corresponding record of a valid SAML token being issued by the identity provider for the environment.
  - Unauthorized modification of user permissions.
  - Unauthorized modifications to the crontab file and/or existence of suspicious file(s) in /var/cron/tabs/ and other locations.

- Files related to this activity have been discovered in /tmp for some, but not all, impacted organizations.
- The command below can assist in finding files that have been associated with this activity. While these files have not been discovered in all environments, their presence may be indicative of actor activity if discovered.

```
find / -type f -name "res*" | grep -E 'res($|\.[a-z]{3})$'
```

Detections:

For additional details including YARA signatures that can be used to detect malware deployed by the actors in this campaign, please see the full report here.

Mitigations:

In the event that you have results from the provided detection methodology, NSA recommends the following steps to mitigate the activity, to the extent applicable in your environment:

- Move all Citrix ADC instances behind a VPN or other capability that requires valid user authentication (ideally multi-factor) prior to being able to access the ADC.
- Isolate the Citrix ADC appliances from the environment to ensure any malicious activity is contained.
- Restore the Citrix ADC to a known good state. Even if you do not have any indications of malicious activity, ensure that your Citrix ADC appliances are running a current version with the latest updates.

Conclusion:

The indicators and context from this analysis can be used by organizations for defensive purposes against this malicious activity. NSA requests that any

additional insights and/or discoveries be shared with the NSA Cybersecurity Collaboration Center in order to enhance understanding of this activity and so that it can be used to improve the overall security posture of the Defense Industrial Base, DoD, and USG.

Reference(s)	Citrix, Citrix, Defense, Citrix, Help Net Security
Report Source(s)	NSA

Sources
Citrix ADC Logs Collection Guide

Critical Security Update Now Available for Citirx ADC, Citrix Gateway

APT5: Citrix ADC Threat Hunting Guidance

Citrix ADC and Citrix Gateway Security Bulletin for CVE-2022-27518

State-Sponsored Attackers Actively Exploiting RCE in Citrix Devices, Patch ASAP (CVE-2022-27518)

Citrix Releases Security Updates in Citrix Gateway and Citrix ADC for CVE-2022-27518

Alert ID 9eb47309

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags MANGANESE, APT5, UNC2630, NSA, Citrix ADC, Citrix Gateway

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**