THREAT BRIEF

Citrix ADC Exploits

Remote Exploits Wreak Havoc on Citrix Infrastructure • Winter 2021

Gartner COOL VENDOR 2020™

Citrix describes its Application Delivery Controller (ADC)—formerly known as NetScaler ADC—as "the most comprehensive application delivery and load balancing solution for monolithic and microservices-based applications." The ADC infrastructure improves the delivery speed and quality of mostly web-based applications for end users. As such, it is a big player in the application delivery controller market, which was valued at $2.4 billion in 2020. This created a large attack surface for remote exploitation, often successful on Citrix ADC installations that are internet-facing.

In December 2019, Citrix began taking steps to mitigate attacks, which kicked off a tough year for the ADC platform. In July 2020, Citrix issued a security update covering a family of related CVE vulnerabilities found in ADC, which achieved different exploitation techniques. These techniques—from cross site scripting (XSS) to information disclosure to unauthenticated web-endpoint access—are often combined in attacks against global ADC infrastructure.

A Flexible Response to an Agile Adversary

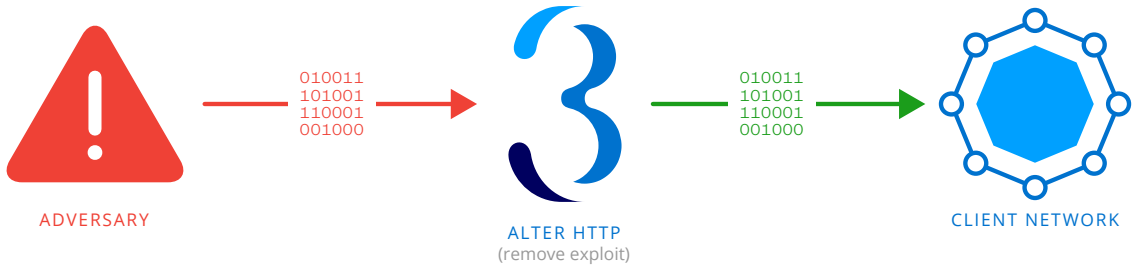
Trinity Cyber detects Citrix ADC exploits by analyzing HTTP traffic at the session level, including both requests and responses. This unusual level of insight grants us unparalleled flexibility to detect both scanning activity as well as remote exploitation attempts. We can therefore find the full range of threat vectors faced by vulnerable ADC infrastructure—from RCE to unauthenticated access.

For example, imagine an adversary scanning for vulnerable ADC instances, implementing remote exploitation through Directory Traversal, and subsequently requesting the results of command execution through a GET request for an XML file. The result of such an attack would be the exposure of private information, from leaked files to sensitive system information to the result of commands run on the ADC controller.

Why a One-Size-Fits-All Response Falls Short

In an ADC attack, stages matter. Law enforcement would behave differently if a criminal were snooping around the front door of a business than if he were pulling money out of the safe. Trinity Cyber responds based on which CVE and stage is detected, with actions ranging from modification of HTTP content to providing non-vulnerable responses to awaiting attackers.

- Unlike traditional cybersecurity technology like a firewall, Trinity Cyber provides options in how to maneuver or act against these various stages.
- This flexibility enables business operations to continue, all while matching the risk tolerances of individual networks.
- Trinity Cyber neutralizes Citrix ADC exploits before they reach vulnerable infrastructure, giving our clients time to react and stopping, rather than responding to, advanced attacks.



sales@trinitycyber.com • (240) 842-9900 • trinitycyber.com

Trinity Cyber