The latest high-severity Citrix vulnerability under attack isn’t easy to fix

Getty Images

reader comments

7 with

A critical vulnerability that hackers have exploited since August, which allows them to bypass multifactor authentication in Citrix networking hardware, has received a patch from the manufacturer. Unfortunately, applying it isn’t enough to protect affected systems.

The vulnerability, tracked as CVE-2023-4966 and carrying a severity rating of 9.8 out of a possible 10, resides in the NetScaler Application Delivery Controller and NetScaler Gateway, which provide load balancing and single sign-on in enterprise networks, respectively. Stemming from a flaw in a currently unknown function, the information-disclosure vulnerability can be exploited so hackers can intercept encrypted communications passing between devices. The vulnerability can be exploited remotely and with no human action required, even when attackers have no system privileges on a vulnerable system.

Citrix released a patch for the vulnerability last week, along with an advisory that provided few details. On Wednesday, researchers from security firm Mandiant said that the vulnerability has been under active exploitation since August, possibly for espionage against professional services,

technology, and government organizations. Mandiant warned that patching the vulnerability wasn't sufficient to lock down affected networks because any sessions hijacked before the security update would persist afterward.

The company wrote:

> *Successful exploitation could result in the ability to hijack existing authenticated sessions, therefore bypassing multi factor authentication or other strong authentication requirements. These sessions may persist after the update to mitigate CVE-2023-4966 has been deployed. Additionally, we have observed session hijacking where session data was stolen prior to the patch deployment, and subsequently used by a threat actor.*
>
> *The authenticated session hijacking could then result in further downstream access based upon the permissions and scope of access that the identity or session was permitted. A threat actor could utilize this method to harvest additional credentials, laterally pivot, and gain access to additional resources within an environment.*

Mandiant provided security guidance that goes well beyond the advice Citrix provided. Specifically:

Advertisement

> *• Isolate NetScaler ADC and Gateway appliances for testing and preparation of patch deployment.*
>
> *Note: If the vulnerable appliances cannot be prioritized for patching, Mandiant recommends that the appliances have ingress IP address restrictions enforced to limit the exposure and attack surface until the necessary patches have been applied.*
>
> *• Upgrade vulnerable NetScaler ADC and Gateway appliances to the latest firmware versions, which mitigate the*

vulnerability.

• Post upgrading, terminate all active and persistent sessions (per appliance).

– Connect to the NetScaler appliance using the CLI.

• To terminate all active sessions, run the following command: kill aaa session -all

• To clear persistent sessions across NetScaler load balancers, run the following command (where is the name of the virtual server / appliance): clear lb persistentSessions

• To clear existing ICA sessions, run the following command: kill icaconnection -all

• Credential Rotation

– Due to the lack of available log records or other artifacts of exploitation activity, as a precaution, organizations should consider rotating credentials for identities that were provisioned for accessing resources via a vulnerable NetScaler ADC or Gateway appliance.

– If there is evidence of suspicious activity or lateral movement within an environment, organizations should prioritize credential rotation for a larger scope of identities if single factor authentication (SFA) remote access is allowed for any resources from the Internet.

• If web shells or backdoors are identified on NetScaler appliances, Mandiant recommends rebuilding the appliances using a clean-source image, including the latest firmware.

Note: If a restoration of an appliance is required using a backup image, the backup configuration should be reviewed to ensure that there is no evidence of backdoors.

• If possible, reduce the external attack exposure and attack

> *surface of NetScaler appliances by restricting ingress access to only trusted or predefined source IP address ranges.*

The advice is warranted given the track record from previous exploitation of critical Citrix vulnerabilities. For example, Citrix disclosed and released a patch for a separate 9.8 vulnerability on July 18. Three days later, according to Internet scans by security organization Shadowserver, more than 18,000 instances had yet to apply the critical update.

By then, according to the US Cybersecurity and Infrastructure Security Administration, the vulnerability was already under active exploit. In the subsequent weeks, Shadowserver and security firms F-Secure and IBM Security Intelligence tracked thousands of exploitations used for credential theft.

What Mandiant’s guidance amounts to is this: If your organization uses either NetScaler ADC or NetScaler Gateway that’s on-premises, you should assume it has been hacked and follow the guidance provided. And yes, that includes patching first.

https://arstechnica.com/?p=1977305