مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Global Password Spraying Attacks Targeting NetScaler Appliances

Tracking #:432316634

Date:16-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Citrix shared mitigations regarding a significant rise in password spraying attacks targeting NetScaler appliances globally.

TECHNICAL DETAILS:

Citrix shared mitigations regarding a significant rise in password spraying attacks targeting NetScaler appliances globally. These attacks, part of a broader industry-wide issue, are characterized by sudden spikes in authentication attempts from diverse IP addresses. The attacks primarily target pre-nFactor endpoints and can lead to operational disruptions, including excessive logging, management CPU overload, and potential appliance instability.

Issue Overview:
Cloud Software Group has observed a surge in password spraying attacks against NetScaler appliances. These attacks target user authentication systems by overwhelming them with large volumes of failed login attempts, which can result in:

- Excessive logging: The high volume of failed logins fills log files, consuming disk space and potentially affecting access to the appliance's management console.
- Management CPU overload: The surge in authentication requests consumes CPU resources, impacting performance, and in some cases triggering High Availability (HA) failover due to missed heartbeats.
- Appliance instability: The authentication module (AAA) may become overwhelmed, causing the appliance to crash.

These attacks are particularly harmful when the targeted appliance is configured to handle typical traffic, which may cause service degradation or failure under the heavy load. Attack traffic usually originates from a wide range of dynamic IP addresses, making traditional mitigation strategies like IP blocking and rate limiting less effective.

Customers utilizing NetScaler Gateway Service are unaffected and do not need to implement mitigations. However, on-premises and cloud-based deployments of NetScaler appliances should urgently apply the recommended actions to protect against these attacks.

Key Recommendations:

- Ensure that multi-factor authentication is enabled for Gateway and the MFA verification factor is configured before the LDAP factor
- Implement responder policies to restrict access to specific FQDNs and block vulnerable endpoints
- Enable Web Application Firewall (WAF) for Gateway protection
- Activate IP reputation feature to automatically block known malicious IP addresses
- Adjust log rotation settings to prevent disk space exhaustion
- Enable reCAPTCHA on NetScaler

RECOMMENDATIONS:

- Implementing the recommended mitigations and maintaining vigilant monitoring are crucial for protecting against these sophisticated and persistent attacks.
- Organizations should prioritize the implementation of multi-factor authentication and the suggested responder policies to enhance their security posture against these evolving threats.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.citrix.com/blogs/2024/12/13/password-spraying-attacks-netscaler-december-2024/