Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

Citrix ADC and Gateway Zero-Day Vulnerability Exploited by APT 5

Date of Publication	Admiralty Code	TA Number
December 14, 2022	A1	TA2022298

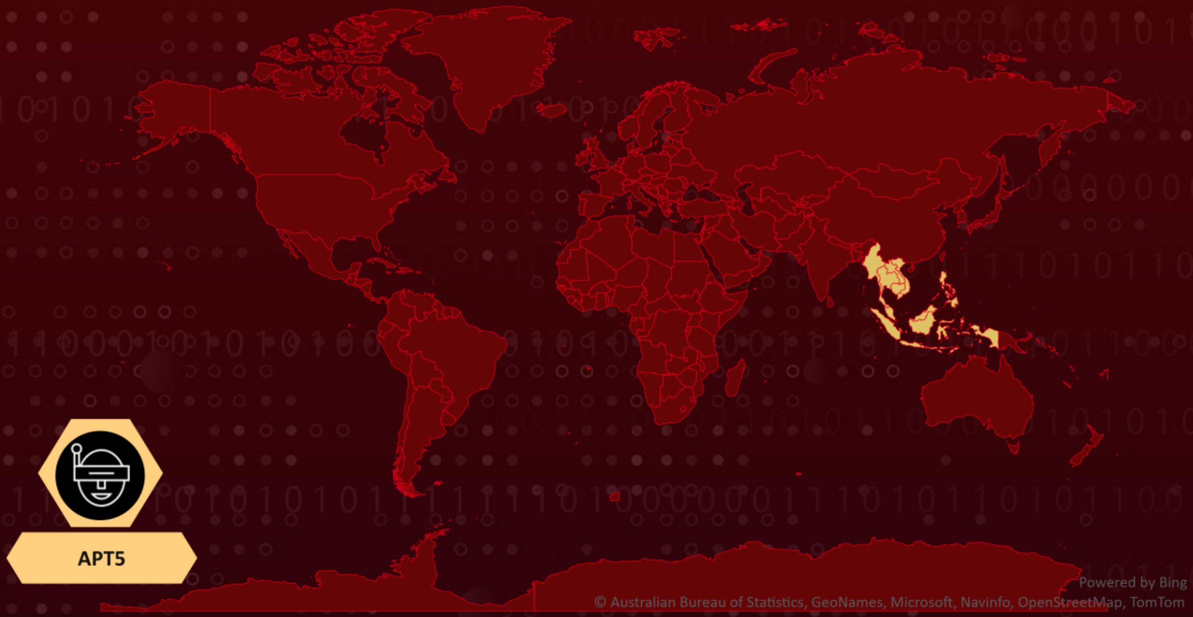
Summary

First appeared: December 13, 2022
Threat Actors: APT5 (aka Bronze Fleetwood, Keyhole Panda, Manganese, UNC2630)
Attack Region: Burma, Brunei, East Timor, Vietnam, Indonesia, Cambodia, Laos, Malaysia, Singapore, Thailand, Philippines
Attack: CVE-2022-27518 was leveraged by APT5 in Citrix Application Delivery Controller (ADC) and Gateway.

CVE

CVE	NAME	PATCH
CVE-2022-27518	Unauthenticated remote arbitrary code execution in Citrix ADC and Gateway	✓

Attack Regions


APT5
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1 The China-based APT5 (aka Bronze Fleetwood, Keyhole Panda, Manganese, UNC2630) threat actors have been actively exploiting a zero-day vulnerability that presents in Citrix Application Delivery Controller (ADC) and Citrix Gateway to gain charge on compromised systems.

#2 The new critical remote arbitrary code vulnerability noted as CVE-2022-27518, could allow an unauthenticated remote hacker to perform arbitrary code execution on the appliance. This vulnerability affects Citrix ADC and Citrix Gateway versions 12.1, 13.0 – 58.32, both configured with a SAML SP or IdP configuration to be impacted. Citrix ADC and Citrix Gateway version 13.1 are not affected.

Recommendations

Security Leaders
Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	T1495 Firmware Corruption	T1204 User Execution
T1588.006 Vulnerabilities	T1190 Exploit Public-Facing Application	TA0011 Command and Control	TA0040 Impact
T1203 Exploitation for Client Execution			

Patch Link

https://www.citrix.com/downloads/citrix-adc/

https://www.citrix.com/downloads/citrix-gateway/

References

https://thehackernews.com/2022/12/hackers-actively-exploiting-citrix-adc.html /

https://www.hivepro.com/citrix-addresses-auth-bypass-flaws-affecting-adc-and-gateway-products/

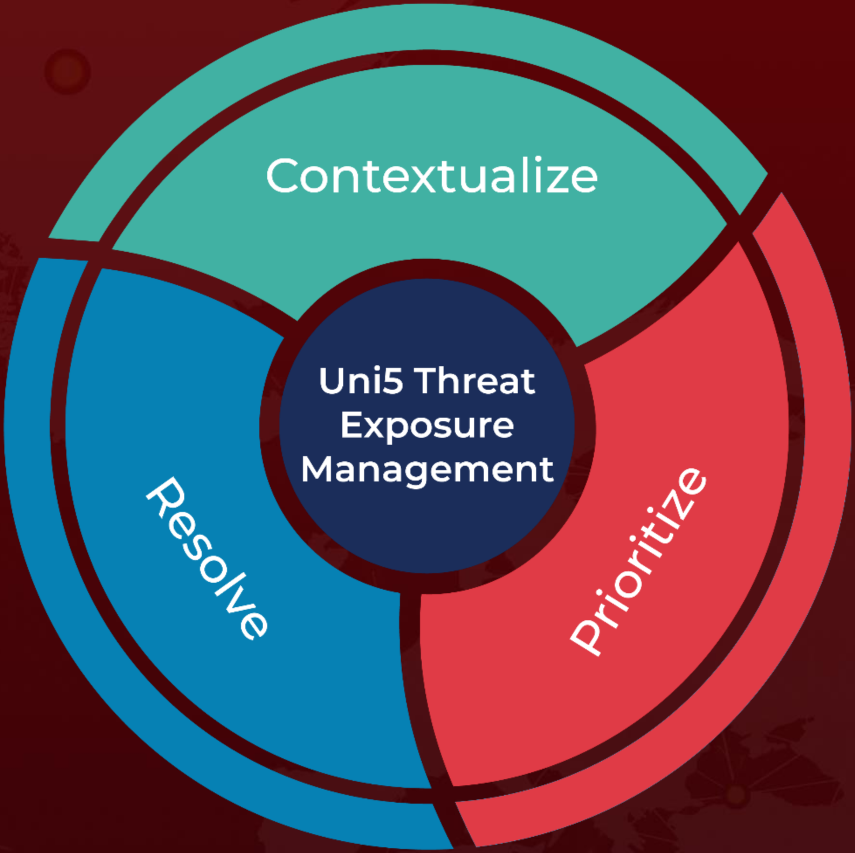
https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518

https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 14, 2022 • 3:45 AM

More at www.hivepro.com