HC3: Alert

March 16, 2022 TLP: White Report: 202203161200

Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability

Executive Summary

The Federal Bureau of Investigation (FBI) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint Cybersecurity Advisory (CSA) to warn organizations that Russian state-sponsored cyber actors have gained network access through exploitation of default MFA protocols and a known vulnerability. As early as May 2021, Russian state-sponsored cyber actors took advantage of a misconfigured account set to default MFA protocols at a non-governmental organization (NGO), allowing them to enroll a new device for MFA and access the victim network. The actors then exploited a critical Windows Print Spooler vulnerability, "PrintNightmare" (CVE-2021-34527) to run arbitrary code with system privileges. Russian state-sponsored cyber actors successfully exploited the vulnerability while targeting an NGO using Cisco's Duo MFA, enabling access to cloud and email accounts for document exfiltration.

Report

Alert AA22-074A - Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability
https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

Impact to HPH Sector

This advisory provides observed tactics, techniques, and procedures, indicators of compromise (IOCs), and recommendations to protect against Russian state-sponsored malicious cyber activity. FBI and CISA urge all organizations to apply the recommendations in the Mitigations section of this advisory, including:

- Enforce MFA and review configuration policies to protect against "fail open" and re-enrollment scenarios.
- Ensure inactive accounts are disabled uniformly across the Active Directory and MFA systems.
- Patch all systems. Prioritize patching for known exploited vulnerabilities.

CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

All organizations should immediately report incidents to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office.

References

Links to additional references and resources can be found in the above referenced report.

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback