Subject: CISA and FBI Release Advisory on Russian State-Sponsored Cyber Activity to Help Protect U.S.

Partners,

Today, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) released this **joint Cybersecurity Advisory** (CSA) to warn organizations that Russian state-sponsored cyber actors have gained network access through exploitation of default multifactor authentication (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 known Windows Print Spooler vulnerability, "PrintNightmare" (CVE-2021-34527) to run arbitrary code and access the victim's Google cloud and email accounts for document exfiltration.

One of the most important security practices to reduce the risk of intrusions remains MFA and every organizations should implement it for all users. MFA should be implemented according to best practices, such as reviewing default configurations and modifying as necessary, to reduce the likelihood that a sophisticated adversary can circumvent this control, as described in this CISA and FBI joint advisory.

Now, more than ever, organizations must put their Shields Up to protect against cyber intrusions. Actions that executives and leaders can implement to help protect against this Russian state-sponsored malicious cyber activity include enforcing MFA and then reviewing configuration policies; ensuring inactive accounts are disabled uniformly across the active directory and MFA systems; and patching all systems, especially prioritizing **known exploited vulnerabilities**.

CISA and FBI encourage all organizations to be cognizant of this threat and apply the recommended mitigations in this advisory. In addition, we encourage all organizations to review our **Shields Up webpage** to find recommended guidance and actions for all organizations, corporate leaders and CEOs, steps to protect yourself and your family, and a technical webpage with guidance from CISA and **Joint Cyber Defense Collaborative** (JCDC) industry partners.

Your support to amplify this advisory through your communications and social media channels is appreciated. CISA and the FBI are posting information about our joint advisory on our social media platforms.

Thank you for your continued support and collaboration.

Cybersecurity and Infrastructure Security Agency

Thank you,

Connect with us at CISA, Facebook, Twitter, LinkedIn, and YouTube

Subscribe to receive CISA alerts and updates

Subscribe to receive DHS information, alerts, & updates

This communication, along with any attachments, is covered by federal and state law governing electronic communications and may contain confidential and legally privileged information. If the reader of this message is not the intended recipient, you are hereby notified that any dissemination, distribution, use or copying of this message is strictly prohibited. If you have received this in error, please reply immediately to the sender and delete this message. Thank you