THREAT BULLETINS

FBI and CISA Release CSA on Russian State-Sponsored Cyber Actors Accessing Networks Misconfigured with Default MFA Protocols

TLP:WHITE

Mar 16, 2022

The United States Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have released a 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.

CISA and FBI encourage all organizations to be cognizant of this threat and apply the recommended mitigations in this advisory. Health-ISAC is releasing this bulletin for your increased security awareness. The full joint CSA, with additional details, can be accessed here.

As early as May of 2021, the FBI observed Russian state-sponsored cyber actors gain access to an NGO, exploit a flaw in default MFA protocols, and move laterally to the NGO’s cloud environment. Russian state-sponsored cyber actors gained initial access to the victim organization via compromised credentials and enrolling a new device in the organization’s Duo MFA. The actors gained the credentials via brute-force password guessing attack, allowing them access to a victim account with a simple, predictable password. The victim account had been un-enrolled from Duo due to a long period of inactivity but was not disabled in the Active Directory. As Duo’s default configuration settings allow for the re-enrollment of a new device for dormant accounts, the actors were able to enroll a new device for this account, complete the authentication requirements, and obtain access to the victim network.

Using the compromised account, Russian state-sponsored cyber actors performed privilege escalation via exploitation of the “PrintNightmare” vulnerability (CVE-2021-34527) to obtain administrator privileges. The actors also modified a domain controller file, c[:]\windows\system32\drivers\etc\hosts, redirecting Duo MFA calls to localhost instead of the Duo server. This change prevented the MFA service from contacting its server to validate MFA login—this effectively disabled MFA for active domain accounts because the default policy of Duo for Windows is to “Fail open” if the MFA server is unreachable.

After effectively disabling MFA, Russian state-sponsored cyber actors were able to successfully authenticate to the victim’s virtual private network (VPN) as non-administrator users and make Remote Desktop Protocol (RDP) connections to Windows domain controllers. The actors ran commands to obtain credentials for additional domain accounts; then using the method described in the previous paragraph, changed the MFA configuration file and bypassed MFA for these newly compromised accounts. The actors leveraged mostly internal Windows utilities already present within the victim network to perform this activity. Using these compromised accounts without

MFA enforced, Russian state-sponsored cyber actors were able to move laterally to the victim’s cloud storage and email accounts and access desired content.

Reference(s)	Infosecurity Magazine, Gov.UK, cisa

Recommendations
The FBI and CISA recommend organizations remain cognizant of the threat of state-sponsored cyber actors exploiting default MFA protocols and exfiltrating sensitive information.

Organizations should:

- Enforce MFA for all users, without exception. Before implementing, organizations should review configuration policies to protect against “fail open” and re-enrollment scenarios.
- Implement time-out and lock-out features in response to repeated failed login attempts.
- Ensure inactive accounts are disabled uniformly across the Active Directory, MFA systems, etc.
- Update software, including operating systems, applications, and firmware on IT network assets in a timely manner. Prioritize patching known exploited vulnerabilities, especially critical and high vulnerabilities that allow for remote code execution or denial-of-service on internet-facing equipment.
- Require all accounts with password logins (e.g., service account, admin accounts, and domain admin accounts) to have strong, unique passwords. Passwords should not be reused across multiple accounts or stored on the system where an adversary may have access.
- Continuously monitor network logs for suspicious activity and unauthorized or unusual login attempts.

FBI and CISA also recommend organizations implement the recommendations listed below to further reduce the risk of malicious cyber activity.

Security Best Practices

- Deploy Local Administrator Password Solution (LAPS), enforce Server Message Block (SMB) Signing, restrict Administrative privileges (local admin users, groups, etc.), and review sensitive materials on domain controller's `SYSVOL` share.
- Enable increased logging policies, enforce PowerShell logging, and ensure antivirus/endpoint detection and response (EDR) are deployed to all endpoints and enabled.
- Routinely verify no unauthorized system modifications, such as additional accounts and Secure Shell (SSH) keys, have occurred to help detect a compromise. To detect these modifications, administrators can use file integrity monitoring software that alerts an administrator or blocks unauthorized changes on the system.

Network Best Practices

- Monitor remote access/ RDP logs and disable unused remote access/RDP ports.
- Deny atypical inbound activity from known anonymization services, including commercial VPN services and The Onion Router (TOR).
- Implement listing policies for applications and remote access that only allow systems to execute known and permitted programs under an established security policy.
- Regularly audit administrative user accounts and configure access control under the concept of least privilege.
- Regularly audit logs to ensure new accounts are legitimate users.
- Scan networks for open and listening ports and mediate those that are unnecessary.
- Maintain historical network activity logs for at least 180 days, in case of a suspected compromise.
- Identify and create offline backups for critical assets.
- Implement network segmentation.
- Automatically update anti-virus and anti-malware solutions and conduct regular virus and malware scans.

Remote Work Environment Best Practices

With an increase in remote work environments and the use of VPN services, the FBI and CISA encourage organizations to implement the following best practices to improve network security:

- Regularly update VPNs, network infrastructure devices, and devices used for remote work environments with the latest software patches and security configurations.
- When possible, implement multi-factor authentication on all VPN connections. Physical security tokens are the most secure form of MFA, followed by authenticator applications. When MFA is unavailable, require employees engaging in remote work to use strong passwords.
- Monitor network traffic for unapproved and unexpected protocols.
- Reduce potential attack surfaces by discontinuing unused VPN servers that may be used as a point of entry for attackers.

User Awareness Best Practices

Cyber actors frequently use unsophisticated methods to gain initial access, which can often be mitigated by stronger employee awareness of indicators of malicious activity. The FBI and CISA recommend the following best practices to improve employee operations security when conducting business:

- Provide end-user awareness and training. To help prevent targeted social engineering and spearphishing scams, ensure that employees and stakeholders are aware of potential cyber threats and delivery methods. Also, provide users with training on information security principles and techniques.
- Inform employees of the risks associated with posting detailed career information to social or professional networking sites.
- Ensure that employees are aware of what to do and whom to contact when they see suspicious activity or suspect a cyberattack, to help quickly and efficiently identify threats and employ mitigation strategies.

Sources

CISA Alert (AA22-074A): Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and “PrintNightmare” Vulnerability

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

InfoSec Magazine: CISA: Fix MFA and Patch Promptly to Stop Russian Attackers

Threat Indicator(s)

IP(s):
45[.]32[.]137[.]94
191[.]96[.]121[.]162
173[.]239[.]198[.]46
157[.]230[.]81[.]39

Alert ID e21961eb

View Alert

Tags Russian APT, Joint Cybersecurity Advisory, MFA Bypass Bugs, Russian Hacker, CISA Alert, MFA bypass, FBI Alert, MFA, Russians, CISA, FBI, Russian

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

FBI The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at www.fbi.gov/contact-us/field. Contact

CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**