JOINT
CYBERSECURITY
ADVISORY

Product ID: AA22-074A
March 15, 2022

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

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.

Multifactor Authentication (MFA): A Cybersecurity Essential

MFA is one of the most important cybersecurity practices to reduce the risk of intrusions—according to industry research, users who enable MFA are up to 99 percent less likely to have an account compromised.

Every organization should enforce MFA for all employees and customers, and every user should sign up for MFA when available.

Organizations that implement MFA should review default configurations and modify as necessary, to reduce the likelihood that a sophisticated adversary can circumvent this control.

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 the following:

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at fbi.gov/contact-us/field-offices. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp/.

- 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.

For more general information on Russian state-sponsored malicious cyber activity, see CISA's Russia Cyber Threat Overview and Advisories webpage. For more information on the threat of Russian state-sponsored malicious cyber actors to U.S. critical infrastructure as well as additional mitigation recommendations, see joint CSA Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure and CISA’s Shields Up Technical Guidance webpage.

For a downloadable copy of IOCs, see [AA22-074A.stix].

TECHNICAL DETAILS

Threat Actor Activity

***Note**: This advisory uses the MITRE ATT&CK® for Enterprise framework, version 10. See appendix A for a table of the threat actors’ activity mapped to MITRE ATT&CK tactics and techniques.*

As early as May 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 [TA0001] to the victim organization via compromised credentials [T1078] and enrolling a new device in the organization’s Duo MFA. The actors gained the credentials [TA0006] via brute-force password guessing attack [T1110.001], 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 [TA0004] via exploitation of the “PrintNightmare” vulnerability (CVE-2021-34527) [T1068] 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 [T1556]. 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. ***Note**: “Fail open” can happen to any MFA implementation and is not exclusive to Duo.*

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 [T1133]. 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 [TA0008] to the victim's cloud storage and email accounts and access desired content.

Indicators of Compromise

Russian state-sponsored cyber actors executed the following processes:

- `ping.exe` – A core Windows Operating System process used to perform the Transmission Control Protocol (TCP)/IP Ping command; used to test network connectivity to a remote host [T1018] and is frequently used by actors for network discovery [TA0007].
- `regedit.exe` – A standard Windows executable file that opens the built-in registry editor [T1112].
- `rar.exe` – A data compression, encryption, and archiving tool [T1560.001]. Malicious cyber actors have traditionally sought to compromise MFA security protocols as doing so would provide access to accounts or information of interest.
- `ntdsutil.exe` – A command-line tool that provides management facilities for Active Directory Domain Services. It is possible this tool was used to enumerate Active Directory user accounts [T1003.003].

Actors modified the `c:\windows\system32\drivers\etc\hosts` file to prevent communication with the Duo MFA server:

- `127.0.0.1 api-<redacted>.duosecurity.com`

The following access device IP addresses used by the actors have been identified to date:

- `45.32.137[.]94`
- `191.96.121[.]162`
- `173.239.198[.]46`
- `157.230.81[.]39`

MITIGATIONS

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.
- Implement security alerting policies for all changes to security-enabled accounts/groups, and alert on suspicious process creation events (`ntdsutil`, `rar`, `regedit`, etc.).

***Note**: If a domain controller compromise is suspected, a domain-wide password reset—including service accounts, Microsoft 365 (M365) synchronization accounts, and `krbtgt`—will be necessary to remove the actors' access. (For more information, see https://docs.microsoft.com/en-us/answers/questions/87978/reset-krbtgt-password.html). Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation.*

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, to include 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 the increased use of remote work environments and 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 cyber actors.

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 cyber incident, to help quickly and efficiently identify threats and employ mitigation strategies.

INFORMATION REQUESTED

All organizations should report incidents and anomalous activity to the FBI via your local FBI field office and/or CISA's 24/7 Operations Center at report@cisa.gov or (888) 282-0870.

APPENDIX A: THREAT ACTOR TACTICS AND TECHNIQUES

See table 1 for the threat actors' tactics and techniques identified in this CSA. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques.

Table 1: Threat Actor MITRE ATT&CK Tactics and Techniques

Tactic	Technique
Initial Access [TA0001]	Valid Accounts [T1078]
Persistence [TA0003]	External Remote Services [T1133]
	Modify Authentication Process [T1556]
Privilege Escalation [TA0004]	Exploitation for Privilege Escalation [T1068]
Defense Evasion [TA0005]	Modify Registry [T1112]
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001]
	OS Credential Dumping: NTDS [T1003.003]
Discovery [TA0007]	Remote System Discovery [T1018]
Lateral Movement [TA0008]	
Collection [TA0009]	Archive Collected Data: Archive via Utility [T1560.001]