APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations

us-cert.cisa.gov/ncas/alerts/aa20-283a

Summary

This joint cybersecurity advisory uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework. See the ATT&CK for Enterprise framework for all referenced threat actor techniques.

Note: the analysis in this joint cybersecurity advisory is ongoing, and the information provided should not be considered comprehensive. The Cybersecurity and Infrastructure Security Agency (CISA) will update this advisory as new information is available.

This joint cybersecurity advisory was written by CISA with contributions from the Federal Bureau of Investigation (FBI).

CISA has recently observed advanced persistent threat (APT) actors exploiting multiple legacy vulnerabilities in combination with a newer privilege escalation vulnerability—CVE-2020-1472—in Windows Netlogon. The commonly used tactic, known as vulnerability chaining, exploits multiple vulnerabilities in the course of a single intrusion to compromise a network or application.

This recent malicious activity has often, but not exclusively, been directed at federal and state, local, tribal, and territorial (SLTT) government networks. Although it does not appear these targets are being selected because of their proximity to elections information, there may be some risk to elections information housed on government networks.

CISA is aware of some instances where this activity resulted in unauthorized access to elections support systems; however, CISA has no evidence to date that integrity of elections data has been compromised. There are steps that election officials, their supporting SLTT IT staff, and vendors can take to help defend against this malicious cyber activity.

Some common tactics, techniques, and procedures (TTPs) used by APT actors include leveraging legacy network access and virtual private network (VPN) vulnerabilities in association with the recent critical CVE-2020-1472 Netlogon vulnerability. CISA is aware of multiple cases where the Fortinet FortiOS Secure Socket Layer (SSL) VPN vulnerability CVE-2018-13379 has been exploited to gain access to networks. To a lesser extent, CISA has also observed threat actors exploiting the MobileIron vulnerability CVE-2020-15505. While these exploits have been observed recently, this activity is ongoing and still unfolding.

After gaining initial access, the actors exploit CVE-2020-1472 to compromise all Active Directory (AD) identity services. Actors have then been observed using legitimate remote access tools, such as VPN and Remote Desktop Protocol (RDP), to access the environment with the compromised credentials. Observed activity targets multiple sectors and is not limited to SLTT entities.

CISA recommends network staff and administrators review internet-facing infrastructure for these and similar vulnerabilities that have or could be exploited to a similar effect, including Juniper CVE-2020-1631, Pulse Secure CVE-2019-11510, Citrix NetScaler CVE-2019-19781, and Palo Alto Networks CVE-2020-2021 (this list is not considered exhaustive).

Click here for a PDF version of this report.

Technical Details

Initial Access

APT threat actors are actively leveraging legacy vulnerabilities in internet-facing infrastructure (*Exploit Public-Facing Application* [T1190], *External Remote Services* [T1133]) to gain initial access into systems. The APT actors appear to have predominately gained initial access via the Fortinet FortiOS VPN vulnerability CVE-2018-13379.

Although not observed in this campaign, other vulnerabilities, listed below, could be used to gain network access (as analysis is evolving, these listed vulnerabilities should not be considered comprehensive). As a best practice, it is critical to patch all known vulnerabilities within internet-facing infrastructure.

- Citrix NetScaler CVE-2019-19781
- MobileIron CVE-2020-15505
- Pulse Secure CVE-2019-11510
- Palo Alto Networks CVE-2020-2021
- F5 BIG-IP CVE-2020-5902

Fortinet FortiOS SSL VPN CVE-2018-13379

CVE-2018-13379 is a path traversal vulnerability in the FortiOS SSL VPN web portal. An unauthenticated attacker could exploit this vulnerability to download FortiOS system files through specially crafted HTTP resource requests.[1]

MobileIron Core & Connector Vulnerability CVE-2020-15505

CVE-2020-15505 is a remote code execution vulnerability in MobileIron Core & Connector versions 10.3 and earlier.[2] This vulnerability allows an external attacker, with no privileges, to execute code of their choice on the vulnerable system. As mobile device management

(MDM) systems are critical to configuration management for external devices, they are usually highly permissioned and make a valuable target for threat actors.

Privilege Escalation

Post initial access, the APT actors use multiple techniques to expand access to the environment. The actors are leveraging CVE-2020-1472 in Windows Netlogon to escalate privileges and obtain access to Windows AD servers. Actors are also leveraging the opensource tools such as Mimikatz and the CrackMapExec tool to obtain valid account credentials from AD servers (*Valid Accounts* [T1078]).

Microsoft Netlogon Remote Protocol Vulnerability: CVE-2020-1472

CVE-2020-1472 is a vulnerability in Microsoft Windows Netlogon Remote Protocol (MS-NRPC), a core authentication component of Active Directory.[3] This vulnerability could allow an unauthenticated attacker with network access to a domain controller to completely compromise all AD identity services (*Valid Accounts: Domain Accounts* [T1078.002]). Malicious actors can leverage this vulnerability to compromise other devices on the network (*Lateral Movement* [TA0008]).

Persistence

Once system access has been achieved, the APT actors use abuse of legitimate credentials (*Valid Accounts* [T1078]) to log in via VPN or remote access services *(External Remote Services* [T1133]) to maintain persistence.

Mitigations

Organizations with externally facing infrastructure devices that have the vulnerabilities listed in this joint cybersecurity advisory, or other vulnerabilities, should move forward with an “assume breach” mentality. As initial exploitation and escalation may be the only observable exploitation activity, most mitigations will need to focus on more traditional network hygiene and user management activities.

Keep Systems Up to Date

Patch systems and equipment promptly and diligently. Establishing and consistently maintaining a thorough patching cycle continues to be the best defense against adversary TTPs. See table 1 for patch information on CVEs mentioned in this report.

Table 1: Patch information for CVEs

Vulnerability	Vulnerable Products	Patch Information

Vulnerability	Vulnerable Products	Patch Information
CVE-2018-13379	• FortiOS 6.0: 6.0.0 to 6.0.4 • FortiOS 5.6: 5.6.3 to 5.6.7 • FortiOS 5.4: 5.4.6 to 5.4.12	Fortinet Security Advisory: FG-IR-18-384
CVE-2019-19781	• Citrix Application Delivery Controller • Citrix Gateway • Citrix SDWAN WANOP	• Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 11.1 and 12.0 • Citrix blog post: security updates for Citrix SD-WAN WANOP release 10.2.6 and 11.0.3 • Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 12.1 and 13.0 • Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway version 10.5
CVE-2020-5902	Big-IP devices (LTM, AAM, Advanced WAF, AFM, Analytics, APM, ASM, DDHD, DNS, FPS, GTM, Link Controller, PEM, SSLO, CGNAT)	F5 Security Advisory: K52145254: TMUI RCE vulnerability CVE-2020-5902
CVE-2019-11510	• Pulse Connect Secure 9.0R1 - 9.0R3.3, 8.3R1 - 8.3R7, 8.2R1 - 8.2R12, 8.1R1 - 8.1R15 • Pulse Policy Secure 9.0R1 - 9.0R3.1, 5.4R1 - 5.4R7, 5.3R1 - 5.3R12, 5.2R1 - 5.2R12, 5.1R1 - 5.1R15	Pulse Secure Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX
CVE-2020-15505	• MobileIron Core & Connector versions 10.3.0.3 and earlier, 10.4.0.0, 10.4.0.1, 10.4.0.2, 10.4.0.3, 10.5.1.0, 10.5.2.0 and 10.6.0.0 • Sentry versions 9.7.2 and earlier, and 9.8.0; • Monitor and Reporting Database (RDB) version 2.0.0.1 and earlier	MobileIron Blog: MobileIron Security Updates Available

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-1631	Junos OS 12.3, 12.3X48, 14.1X53, 15.1, 15.1X49, 15.1X53, 17.2, 17.3, 17.4, 18.1, 18.2, 18.3, 18.4, 19.1, 19.2, 19.3, 19.4, 20.1	Juniper Security Advisory JSA11021
CVE-2020-2021	PAN-OS 9.1 versions earlier than PAN-OS 9.1.3; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 8.1 versions earlier than PAN-OS 8.1.15, and all versions of PAN-OS 8.0 (EOL)	Palo Alto Networks Security Advisory for CVE-2020-2021
CVE-2020-1472	• Windows Server 2008 R2 for x64-based Systems Service Pack 1 • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) • Windows Server 2012 • Windows Server 2012 (Server Core installation) • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2019 (Server Core installation) • Windows Server, version 1903 (Server Core installation) • Windows Server, version 1909 (Server Core installation) • Windows Server, version 2004 (Server Core installation)	Microsoft Security Advisory for CVE-2020-1472

Comprehensive Account Resets

If there is an observation of CVE-2020-1472 Netlogon activity or other indications of valid credential abuse detected, it should be assumed the APT actors have compromised AD administrative accounts, the AD forest should not be fully trusted, and, therefore, a new forest should be deployed. Existing hosts from the old compromised forest cannot be migrated in without being rebuilt and rejoined to the new domain, but migration may be done through “creative destruction,” wherein as endpoints in the legacy forest are decommissioned, new ones can be built in the new forest. This will need to be completed on on-premise as well as Azure-hosted AD instances.

Note that fully resetting an AD forest is difficult and complex; it is best done with the assistance of personnel who have successfully completed the task previously.

It is critical to perform a full password reset on all user and computer accounts in the AD forest. Use the following steps as a guide.

1. Create a temporary administrator account, and use this account only for all administrative actions
2. Reset the Kerberos Ticket Granting Ticket (`krbtgt`) password [4]; this must be completed before any additional actions (a second reset will take place in step 5)
3. Wait for the krbtgt reset to propagate to all domain controllers (time may vary)
4. Reset all account passwords (passwords should be 15 characters or more and randomly assigned):
    1. User accounts (forced reset with no legacy password reuse)
    2. Local accounts on hosts (including local accounts not covered by Local Administrator Password Solution [LAPS])
    3. Service accounts
    4. Directory Services Restore Mode (DSRM) account
    5. Domain Controller machine account
    6. Application passwords
5. Reset the `krbtgt` password again
6. Wait for the `krbtgt` reset to propagate to all domain controllers (time may vary)
7. Reboot domain controllers
8. Reboot all endpoints

The following accounts should be reset:

- AD Kerberos Authentication Master (2x)
- All Active Directory Accounts
- All Active Directory Admin Accounts
- All Active Directory Service Accounts
- All Active Directory User Accounts
- DSRM Account on Domain Controllers
- Non-AD Privileged Application Accounts
- Non-AD Unprivileged Application Accounts
- Non-Windows Privileged Accounts
- Non-Windows User Accounts
- Windows Computer Accounts
- Windows Local Admin

CVE-2020-1472

To secure your organization's Netlogon channel connections:

- **Update all Domain Controllers and Read Only Domain Controllers**. On August 11, 2020, Microsoft released software updates to mitigate CVE-2020-1472. Applying this update to domain controllers is currently the only mitigation to this vulnerability (aside from removing affected domain controllers from the network).
- **Monitor for new events, and address non-compliant devices** that are using vulnerable Netlogon secure channel connections.
- **Block public access to potentially vulnerable ports**, such as 445 (Server Message Block [SMB]) and 135 (Remote Procedure Call [RPC]).

To protect your organization against this CVE, follow advice from Microsoft, including:

- Update your domain controllers with an update released August 11, 2020, or later.
- Find which devices are making vulnerable connections by monitoring event logs.
- Address non-compliant devices making vulnerable connections.
- Enable enforcement mode to address CVE-2020-1472 in your environment.

VPN Vulnerabilities

Implement the following recommendations to secure your organization's VPNs:

- **Update VPNs, network infrastructure devices, and devices** being used to remote into work environments with the latest software patches and security configurations. See CISA Tips Understanding Patches and Software Updates and Securing Network Infrastructure Devices. Wherever possible, enable automatic updates. See table 1 for patch information on VPN-related CVEs mentioned in this report.
- **Implement multi-factor authentication (MFA) on all VPN connections to increase security**. Physical security tokens are the most secure form of MFA, followed by authenticator app-based MFA. SMS and email-based MFA should only be used when no other forms are available. If MFA is not implemented, require teleworkers to use strong passwords. See CISA Tips Choosing and Protecting Passwords and Supplementing Passwords for more information.

Discontinue unused VPN servers. Reduce your organization's attack surface by discontinuing unused VPN servers, which may act as a point of entry for attackers. To protect your organization against VPN vulnerabilities:

- **Audit** configuration and patch management programs.
- **Monitor** network traffic for unexpected and unapproved protocols, especially outbound to the internet (e.g., Secure Shell [SSH], SMB, RDP).
- **Implement** MFA, especially for privileged accounts.
- **Use** separate administrative accounts on separate administration workstations.
- **Keep** software up to date. Enable automatic updates, if available.

How to uncover and mitigate malicious activity

- **Collect and remove** for further analysis:
  Relevant artifacts, logs, and data.
- **Implement** mitigation steps that avoid tipping off the adversary that their presence in the network has been discovered.
- **Consider** soliciting incident response support from a third-party IT security organization to:
  - Provide subject matter expertise and technical support to the incident response.
  - Ensure that the actor is eradicated from the network.
  - Avoid residual issues that could result in follow-up compromises once the incident is closed.

Resources

- CISA VPN-Related Guidance
- CISA Infographic: Risk Vulnerability And Assessment (RVA) Mapped to the MITRE ATT&CK FRAMEWORK
- National Security Agency InfoSheet: Configuring IPsec Virtual Private Networks
- CISA Joint Advisory: AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity
- CISA Activity Alert: AA20-073A: Enterprise VPN Security
- CISA Activity Alert: AA20-031A: Detecting Citrix CVE-2019-19781
- CISA Activity Alert: AA20-010A: Continued Exploitation of Pulse Secure VPN Vulnerability
- **Cybersecurity Alerts and Advisories**: Subscriptions to CISA Alerts and MS-ISAC Advisories

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat.

For any questions related to this report or to report an intrusion and request resources for incident response or technical assistance, please contact:

- CISA (888-282-0870 or Central@cisa.dhs.gov), or
- The FBI through the FBI Cyber Division (855-292-3937 or CyWatch@fbi.gov) or a local field office

DISCLAIMER

This information is provided "as is" for informational purposes only. The United States Government does not provide any warranties of any kind regarding this information. In no event shall the United States Government or its contractors or subcontractors be liable for any damages, including but not limited to, direct, indirect, special or consequential damages,

arising out of, resulting from, or in any way connected with this information, whether or not based upon warranty, contract, tort, or otherwise, whether or not arising out of negligence, and whether or not injury was sustained from, or arose out of the results of, or reliance upon the information.

The United States Government does not endorse any commercial product or service, including any subjects of analysis. Any reference to specific commercial products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply their endorsement, recommendation, or favoring by the United States Government.

References

Revisions

October 9, 2020: Initial Version

October 11, 2020: Updated Summary

October 12, 2020: Added Additional Links

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.