Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials

Understand The Threat



Nation state level exploitation is seen in the wild

Vulnerability requires password-based access to the web interface (requires additional means for initial access)

Vulnerability also allows attackers to execute Linux commands (if attacker does exploit, enables persistence potentials)

Understand the Relevance



Identify if networks use vulnerable VMware Access or Identity Manager versions

Identify if customer or partner networks use affected products

S Prioritize the Response



Identify if sensitive data can be accessed when using the vulnerable products

Assess the risk if that data is accessed

Identify efficient patch implementation needs

- Complete additional actions as warranted
- Check server logs
- Check and update authentication service configurations
- Use multi-factor authentication for security credential services



For more information on how to identify and mitigate this threat, refer to NSA's cybersecurity product "Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials" available on NSA.gov/cybersecurity-guidance.