Russian SVR Targets U.S. and Allied Networks

Executive summary

Russian Foreign Intelligence Service (SVR) actors (also known as APT29, Cozy Bear, and The Dukes) frequently use publicly known vulnerabilities to conduct widespread scanning and exploitation against vulnerable systems in an effort to obtain authentication credentials to allow further access. This targeting and exploitation encompasses U.S. and allied networks, including national security and government-related systems.

Recent Russian SVR activities include compromising SolarWinds® Orion® software updates,[1] targeting COVID-19 research facilities through deploying WellMess malware,[2] and leveraging a VMware® vulnerability that was a zero-day at the time for follow-on Security Assertion Markup Language (SAML) authentication abuse.[3] SVR cyber actors also used authentication abuse tactics following SolarWinds-based breaches.[4] [5]

The SVR has exploited—and continues to successfully exploit—software vulnerabilities to gain initial footholds into victim devices and networks, to include:

- CVE-2018-13379 Fortinet®[2]
- CVE-2019-9670 Zimbra®[2]
- CVE-2019-11510 Pulse Secure®[2]
- CVE-2019-19781 Citrix®[2]
- CVE-2020-4006 VMware®[3]

The National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) previously shared mitigations to defend against exploitation of these vulnerabilities. Knowing the tradecraft that nation-state cyber actors use along with relevant response actions will enable network defenders to focus on mitigating the vulnerabilities and techniques, enabling more comprehensive protection against adversary compromise.

Detailed vulnerabilities and mitigations

NSA, CISA, and FBI are aware that United States Government, critical infrastructure (including Defense Industrial Base), and allied networks are consistently scanned, targeted, and exploited by Russian state-sponsored cyber actors. NSA, CISA, and FBI recommend that critical system owners prioritize the following mitigation actions to mitigate the loss of sensitive information that could impact U.S. policies, strategies, plans, ongoing operations, and competitive advantage. Additionally, due to the various systems and networks that could be impacted outside of these sectors, NSA, CISA, and FBI recommend that the following mitigations be prioritized for action by all network defenders.

The techniques leveraged by SVR actors include[1]:

- Exploiting public-facing applications (T1190[2])
- Leveraging external remote services (T1133)
- Compromising supply chains (T1195)
- Using valid accounts (T1078)
- Exploiting software for credential access (T1212)
- Forging web credentials: SAML tokens (T1606.002)

While some vulnerabilities have specific additional mitigations below, the following general mitigations apply:

- Keep systems and products updated and patch as soon as possible after patches are released since many actors exploit numerous vulnerabilities.[3]
- Expect that the risk from data stolen or modified (including credentials, accounts, and software) before a device was patched will not be alleviated by patching or simple remediation actions. Assume that a breach will happen, enforce least-privileged access, and make password changes and account reviews a regular practice.[4]
- Disable external management capabilities and set up an out-of-band management network.[5]
- Block obsolete or unused protocols at the network edge and disable them in device configurations.[6]
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce exposure of the internal network.[7]
- Enable robust logging of Internet-facing services and authentication functions. Continuously hunt for signs of compromise or credential misuse, particularly within cloud environments.[8]
- Adopt a mindset that compromise happens: prepare for incident response activities, only communicate about breaches on out-of-band channels, and take care to uncover a breach's full scope before remediating.[9]

The following is a list of specific Common Vulnerabilities and Exposures (CVEs) being actively exploited by SVR actors, a description of the vulnerability, and the recommended mitigations.

CVE Number	Vulnerability Description	Prior Cybersecurity Guidance
CVE-2018-13379	*In Fortinet Secure Sockets Layer (SSL) Virtual Private Network (VPN) web portals, an Improper Limitation of a Pathname to a Restricted Directory ("Path Traversal") allows an unauthenticated attacker to download system files via special crafted HTTP resource requests.*	Advisory: APT29 target COVID-19 vaccine development (U/OO/152680-20) Mitigating Recent VPN Vulnerabilities (U/OO/196888-19)
Affects: Fortinet FortiOS 6.0.0 to 6.0.4, 5.6.3 to 5.6.7 and 5.4.6 to 5.4.12		
CVE-2019-9670	*In Synacor Zimbra Collaboration Suite, the mailboxd component has an XML External Entity injection (XXE) vulnerability.*	Advisory: APT29 target COVID-19 vaccine development (U/OO/152680-20)
Affects: Synacor Zimbra Collaboration Suite 8.7.x before 8.7.11p10.		

[1] Refer to CISA Alert: Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (AA20-352A) for more techniques.
[2] T1190 and similar references are MITRE® ATT&CK® techniques.
[3] Refer to Update and Upgrade Software Immediately (U/OO/181147-19).
[4] Refer to Defend Privileges and Accounts (U/OO/181857-19) and the "assume breach" principle of CSI – Embracing a Zero Trust Security Model (U/OO/115131-21).
[5] Refer to Perform Out-of-Band Network Management (U/OO/169570-20).
[6] Refer to Hardening Network Devices (U/OO/171339-16), Outdated Software and Protocols (U/OO/802041-16), and Outdated Network Devices and Unsecured Protocols (U/OO/802587-16).
[7] Refer to Segment Networks and Deploy Application-Aware Defenses (U/OO/184967-19).
[8] Refer to CISA Alert Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments (AA21-008A).
[9] Refer to CISA Alert: Technical Approaches to Uncovering and Remediating Malicious Activity (AA20-245A).

CVE Number	Vulnerability Description	Prior Cybersecurity Guidance
CVE-2019-11510	*In Pulse Secure VPNs, an unauthenticated remote attacker can send a specially crafted Uniform Resource Identifier (URI) to perform an arbitrary file read.*	Advisory: APT29 target COVID-19 vaccine development (U/OO/152680-20) Mitigating Recent VPN Vulnerabilities (U/OO/196888-19)
Affects: Pulse Connect Secure (PCS) 8.2 before 8.2R12.1, 8.3 before 8.3R7.1, and 9.0 before 9.0R3.4.		
CVE-2019-19781	*Citrix® Application Delivery Controller (ADC) and Gateway allow directory traversal.*	Advisory: APT29 target COVID-19 vaccine development (U/OO/152680-20) Detect and Prevent Web Shell Malware (U/OO/134094-20) Mitigate CVE-2019-19781 (U/OO/103100-20)
Affects: Citrix ADC and Gateway versions before 13.0.47.24, 12.1.55.18, 12.0.63.13, 11.1.63.15 and 10.5.70.12 and SD-WAN WANOP 4000-WO, 4100-WO, 5000-WO, and 5100-WO versions before 10.2.6b and 11.0.3b.		
CVE-2020-4006	*VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector have a command injection vulnerability.*	Russian State-Sponsored Actors Exploiting Vulnerability in VMware Workspace ONE Access Using Compromised Credentials (U/OO/195076-20) Perform Out-of-Band Network Management (U/OO/169570-20)
Affects: VMware One Access 20.01 and 20.10 on Linux, VMware Identity Manager 3.3.1 - 3.3.3 on Linux, VMware Identity Manager Connector 3.3.1 - 3.3.3 and 19.03, VMware Cloud Foundation 4.0 - 4.1, and VMware Vrealize Suite Lifecycle Manager 8.x.		

Works cited

[1] White House (2021), White House Public Attribution Statement. Available at: https://www.whitehouse.gov/briefing-room/

[2] National Cyber Security Centre (UK), Communications Security Establishment (Canada), National Security Agency, and Cybersecurity and Infrastructure Security Agency (2020), Advisory: APT29 targets COVID-19 vaccine development (U/OO/152680-20). Available at: https://www.nsa.gov/cybersecurity-guidance

[3] National Security Agency (2020), Russian State-Sponsored Actors Exploiting Vulnerability in VMware Workspace ONE Access Using Compromised Credentials (U/OO/195076-20). Available at: https://www.nsa.gov/cybersecurity-guidance

[4] National Security Agency (2020), Detecting Abuse of Authentication Mechanisms (U/OO/198854-20). Available at: https://www.nsa.gov/cybersecurity-guidance

[5] Federal Bureau Of Investigation, Cyber Division (2020), Advanced Persistent Threat Actors Leverage SolarWinds Vulnerabilities (PIN 20201222-001). Available at: https://www.ic3.gov/Media/News/2020/201229.pdf

Disclaimer of endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed by NSA, CISA and FBI in furtherance of their respective cybersecurity missions, including their responsibilities to identify and disseminate information about threats to U.S. Government and critical infrastructure information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Trademarks

SolarWinds® and SolarWinds Orion® are registered trademark of SolarWinds Worldwide, LLC. • VMware®, VMware Workspace ONE®, VMware Identity Manager (vIDM)®, VMware Access®, VMware Cloud Foundation®, and VMware vRealize Suite Lifecycle Manager® are registered trademarks of VMware, Inc. • Fortinet® is a registered trademark of Fortinet, Inc. • Zimbra® is a registered trademark of Synacor, Inc. • Pulse Secure® is a registered trademark of Pulse Secure, LLC. • Citrix® is a registered trademark of Citrix Systems, Inc.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov
- FBI National Press Office, 202-324-3691, npo@fbi.gov