DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

DCSA-SIB-0040-21 Dissemination Date: 5 May 2021 Date of Information: 3 May 2021

Cyber Shared Indicator Bulletin (SIB)

(U) Update 1 of Likely Chinese APT using Pulse Secure VPN Vulnerability to Attack Cleared Contractors

(U) WARNING: This product may contain information associated with United States Persons (USPER) as defined by Executive Order (EO) 12333 and Department of Defense Manual (DoDM) 5240.01. Such information should be handled and protected in accordance with applicable Intelligence Oversight rules by persons and organizations subject to those rules. The Defense Counterintelligence Security Agency (DCSA) collects, retains, and disseminates USPER Information (USPI) in accordance with all applicable laws, directives, and policies. Should you require minimized USPI, contact Eric Kutchins, Commercial 571-305-6592, Eric.d.kutchins.civ@mail.mil.

(U) WARNING: As stated in the National Industrial Security Program Operating Manual, page 5-5-1, paragraph 5-511. Disclosure to the Public. Contractors shall not disclose classified or unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the Contract Security Classification Specification for the contract or as otherwise specified by the Government Contracting Authority (GCA). The information provided in this bulletin is Controlled Unclassified Information (CUI) and is NOT publically releasable information. Release outside of official security, cyber, and counterintelligence channels within the receiving facility or company requires the recipient to send a release request to DCSA. As defined in DoDM 5200.01, Volume 3, DoD Information Security Program, unauthorized disclosure is the communication or physical transfer of classified or CUI to an unauthorized recipient. The information below is provided to cleared industry for use in the protection of UNCLASSIFIED information resident on unclassified networks pertaining to CLASSIFIED programs.

(U) SUMMARY

(U) DCSA recently received reporting of additional Cleared Contractor (CC) compromises involving Pulse Secure Virtual Private Network (VPN) vulnerabilities. Previously DCSA-SIB-0038-21 highlighted that a U.S. cyber security research firm identified a likely Chinese Advanced Persistent Threat (APT) cyber actor targeting U.S. Defense Industrial Base (DIB) networks, which includes members of cleared industry, via a new zero day targeting Pulse Secure VPN appliances. A combination of prior vulnerabilities and a previously unknown vulnerability discovered in April 2021, CVE-2021-22893, are responsible for the initial infection vector. Once compromised, the cyber actors harvest credentials from various Pulse Secure VPN login flows, which ultimately allows the actor to use legitimate account credentials to move laterally into the affected environments.

(CUI) Recent compromised CC reports indicate that initial entry vector via Pulse Secure VPN vulnerabilities enables threat actors to install a wide variety of additional malware on compromised networks and systems gaining persistence, unauthorized access to network resources such as email servers, and other remote access capabilities. Threat actors using Pulse Secure VPN vulnerabilities have in multiple instances also used methods to obfuscate their activity throughout their successful compromise activities, to include deletion of server logs, deletion of custom code used on servers, and deletion of uploaded files used to install malware.

(U) DETAILS

(CUI) Intrusions targeting defense, government, and financial organizations around the world were detected late 2020 through early 2021. In each intrusion, the earliest evidence of attacker activity traced back to Dynamic Host Configuration Protocol (DHCP) IP address ranges belonging to Pulse Secure VPN appliances in the affected environment. However, it is suspected some intrusions were due to the exploitation of previously disclosed Pulse Secure vulnerabilities from 2019 and 2020 while other intrusions were due to the exploitation of CVE-2021-22893. For full technical details of exploitation tactics, techniques and procedures (TTP), and detection/remediation tools please refer to DCSA-SIB-0038-21.

(U) The Cybersecurity and Infrastructure Security Agency (CISA) recently responded to an APT actor's long-term compromise of an entity's enterprise network, which began in at least March 2020. The threat actor connected to the entity's network via a Pulse Secure VPN appliance, moved laterally to its SolarWinds Orion server, installed malware referred to by security researchers as SUPERNOVA (a .NET webshell), and collected credentials.

(CUI) Additionally, DCSA recently received reports form five separate CC's that their systems were affected by exploitation of Pulse Secure VPN vulnerabilities. The dates of compromise ranged November 2020 to Present. In one such instance threat actors compromised Pulse Secure VPN servers in November 2020 and created an admin level account that was successfully in use on and off until 8 March 2021. The threat actor used their permissions to access user email resources, create custom sign in pages, and modify Roles and Realms within the Pulse config, and potentially other activities that have not yet been uncovered in the forensics process. The APT attempted to obfuscate their activity by deleting their custom pages, deleting zip files used in their exploitation, and deleting server log data for instances where they were active.

(U) Pulse Secure VPN has released a patch for the above mentioned vulnerabilities, it is highly recommended that any CC running Pulse Secure VPN appliances installs the patch. Patching the vulnerability will negate threat actor ability to exploit the vulnerability in the future. However, it will not remediate compromises that have already occurred using the vulnerability prior to patching.

(U) TECHNICAL DETAILS

(U) Use of a Pulse Secure VPN vulnerability allows threat actors to establish new user roles, permissions, and gain network persistence by installing a wide range of malware on systems and network connected devices.

(CUI) A CC recently ran the Pulse Secure Integrity Checker application, discovering that files had been modified on their two Pulse Secure clusters; the cluster that handles access to specific websites on the network perimeter, and the cluster that handles web-based access to internal resources. On 2 November 2020, multiple IPs were seen authenticating to a CC's perimeter Pulse Secure appliance web portal using the built-in local admin account (IVEADMIN). The local account was used on and off successfully for some time, up until 8 March 2021. During this period, there was evidence that Roles and Realms were modified within the Pulse config, and internal resource shares may have been accessed due to the creation of Pulse Secure bookmarks, pointing to Windows share locations, as well as bookmarks to the CCs RSA servers.

(CUI) The threat actor was also seen creating a custom sign-in page, then executing tcpdump on the appliance. Around the time tcpdump was running, a ZIP file was created by the actor. Afterwards, the actor logged back in and deleted the sign-in page and ZIP file. On 7 December 2020, there was a successful authentication with a user account to a second Pulse Secure appliance web portal, from the same IP previously seen authenticating to the Pulse Secure with IVEADMIN. It appears email resources were accessed for this user. It also appears that sections of logs are missing from the appliances indicative of APT obfuscation efforts.

(CUI) The IP addresses used by the threat actors in this attack are as follows:

81.151.38.243
216.196.79.223
76.72.43.198
174.67.97.170
24.117.18.111
31.54.182.205
76.72.43.198
128.125.146.117
71.61.214.247
41.210.159.108
167.99.169.182

CUI

(CUI) On 16 April 2021, a CC identified one non-production Pulse Secure VPN device used to pilot new installations had 2 mismatch files. All other Pulse Secure devices, which are used to provide remote access to users, came back clean. That same day CC uploaded the 2 mismatch files to Pulse Secure for decryption and analysis. The Pulse Secure forensics team concluded that the files from the CCs pilot device contained malicious code. However, the Pulse Secure forensic team concluded that the code looked garbled and un-useable in its current form. Further forensic analysis is under way. The garbling of code in the above instance is likely indicative of APT obfuscation efforts after successful compromises.

(U) From at least March 2020 through February 2021, CISA determined a threat actor connected to a CC via the CCs Pulse Secure VPN appliance. The threat actor connected via the U.S.-based residential IP addresses listed below, which allowed them to masquerade as teleworking employees. (Note: these IP addresses belong to routers that are all similar models; based on this activity, CISA suspects that these routers were likely exploited by the threat actor.)

207.89.9.153
24.140.28.90
24.117.18.111

UNCLASSIFIED

(U) The threat actor authenticated to the VPN appliance through several user accounts, none of which had multi-factor authentication (MFA) enabled. Once authenticated to the VPN appliance, the threat actor initiated a VPN connection to the environment. The media access control (MAC) address of the threat actor's machine as recorded in the VPN appliance logs indicates use of a virtual machine. The threat actor then moved laterally to the entity's SolarWinds Orion and established persistence by using a PowerShell script to decode and install SUPERNOVA, Server Software Component: Web Shell. The SUPERNOVA webshell allows a remote operator to dynamically inject C# source code into a web portal provided via the SolarWinds software suite. The injected code is compiled and directly executed in memory. For more information on SUPERNOVA, refer to MAR-10319053-1.v1 - SUPERNOVA.

(U) The threat actor was able to dump credentials from the SolarWinds appliance via two methods. First, they used Export-PfxCertificate to gather cached credentials used by the SolarWinds appliance server and network monitoring. The private key certificate must have been marked as exportable; either the threat actor was able to change or bypass that property prior, or the affected entity mistakenly marked the certificate exportable. Second, the threat actor placed a copy of procdump.exe disguised as the entity's logging infrastructure, splunklogger.exe on the SolarWinds Orion server. The threat actor used this tool and the system-level access to dump Local Security Authority Subsystem Service (LSASS) memory to obtain additional credentials. Once the credentials were dumped, the threat actor placed them in the c:\inetpub\SolarWinds\ja\license.txt directory, and the threat actor made a GET request to the entity's internet information services (IIS) server to Exfiltrate. The threat actor deleted the IIS logs for the date in question.

(U) CISA believes the logs would have likely revealed the threat actor exploited CVE-2020-10148, an authentication bypass vulnerability in SolarWinds Orion Application Programming Interface (API) that allows a remote attacker to execute API commands. CISA believes the threat actor leveraged CVE-2020-10148 to bypass the authentication to the SolarWinds appliance and then used SolarWinds Orion API ExecuteExternalProgram to run commands with the same privileges the SolarWinds appliance was running (in this case SYSTEM). CISA had not observed the threat actor using privileged accounts prior to the credential dumps, and the account being used to connect to the SolarWinds appliance (via VPN) did not have sufficient privilege to access it. The PowerShell process that initiated the credential harvesting and installation of SUPERNOVA was a child process of the solarwindsbusinesslayer.exe process. Two GET requests were logged in the following day's log, with the internal Dynamic Host Configuration Protocol (DHCP) address given to the threat actor's machine by the VPN appliance minutes after the exploitation, suggesting the threat actor was interacting with the SolarWinds web application. (Note: although the threat actor likely exploited CVE-2020-10148, it could have also exploited another API authentication bypass or remote code execution (RCE) vulnerability.)

(U) Several weeks later, the threat actor connected again via the VPN appliance and attempted to use credentials gained from the SolarWinds appliance. The threat actor connected to one machine via Server Message Block (SMB) (Transmission Control Protocol [TCP] port 445) and then attempted to login to an additional workstation. No additional activity was observed during this session.

(U) On another occasion, the threat actor connected to the environment via the VPN and used Windows Management Instrumentation (WMI) to remotely launch a tasklist to determine the process ID for the LSASS process. Then the threat actor, via WMI, launched procdump.exe, which was disguised as wininit.exe. After this, the threat actor placed and ran winrar, which was also disguised as wininit.exe, to archive credentials. CISA observed the disguised wininit.exe commands on two separate machines—one server and one workstation. The commands executed were:

- (U) cmd /c tasklist /vc:\windows\temp\TS_85ET.tmp
- (U) procdump.exe:
- (U) cmd.exe c:\windows\temp\wininit.exe -accepteula -ma 992 c:\windows\temp\TS_9D3C.tmp
- (U) winrar.exe:
- (U) c:\windows\temp\wininit.exe a c:\windows\temp\googleupdate.tmp -hpJimJameJump c:\windows\temp\TS_9D3C.tmp.dmp

(U) Please see the CISA report ar21-112a for security recommendations that could help prevent compromises such as the example above.

(U) Finally, DCSA has received information that a tar file containing STEADYPULSE and PULSECHECK are being used in conjunction with Pulse Secure VPN vulnerability compromises. Hash values for the malicious files are in the table below.

MD5:	97916393ad3eea996ea6f826e4865ee3
MD5:	8073bdf06730e1db35de0717f031972e
MD5:	e7e2f79ade6f198c5d9707b6f94a9a41

UNCLASSIFIED

(CUI) Chinese APTs are likely using unpatched Pulse Secure VPN vulnerabilities in their attacks against CCs to compromise and gain initial access to CC networks. Once a CC network is compromised via Pulse Secure VPN vulnerabilities threat actors are able to move laterally through the affected networks, establishing persistence and upgrading user permissions and roles, ultimately gaining access to files and resources of interest. Patching likely does nothing to mitigate threat actor access to an already compromised system as a competent APT will enable other vectors of entry to grant themselves persistence on the affected CCs network. Cyber forensic analysis should be conducted on the entirety of the network and any devices accessed by threat actors should likely be removed and reimaged. Affected CCs should also check for new or modified user accounts with inappropriate access levels. For additional guidance on how to check for compromise reference the Pulse Connect Secure Integrity Tool. For additional information on Pulse Secure VPN compromises please reference previous DCSA-SIB-0038-21.

(U) ADDITIONAL INFORMATION

(U) This bulletin should only be released to company employees who need the information for network security duties and should not be disseminated without DCSA permission. Further dissemination of DCSA cyber threat products must be granted on a case-by-case basis to prevent unauthorized public disclosure.

(U) Companies should follow established internal procedures if they suspect any malicious activity and promptly report the incident in accordance with existing policies, regulations, and agreements. The DCSA cyber threat products are not intended to serve as definitive block lists. DCSA does not provide recommendations or advice regarding protections of information systems processing unclassified information. Product recipients must decide how to use the information contained in this document. Each company must weigh possible risks against operational requirements when determining any block list implementation.

(U) This product contains information derived from DCSA analysis or reports from multiple sources, including National Industrial Security Program (NISP) participants and U.S. Government agencies. DCSA provides this product to cleared contractor security professionals to facilitate cyber threat awareness for their classified and unclassified networks and to aid in identifying and developing appropriate actions, priorities, and follow-on measures. DCSA receives, analyzes, and disseminates the information in this product in accordance with its assigned missions. The intrusion behavior descriptions and general methodologies cited in this bulletin may be used to monitor for and detect traffic of interest; however, no action should be taken against any of the IP addresses or hostnames. Users should note that information contained in this product does not, unless otherwise noted, contain finished intelligence.

(U) **Reporting Notice & Feedback:** DCSA CI CD prepared this product. Please contact DCSA CD with any technical questions related to these products at DCSA.CYBERCI@mail.mil. In the event that new or reportable cyber/counterintelligence information comes to light; please contact your local DCSA field office and agent.

(U) REFERENCES

(U) **WARNING:** This product may contain information associated with USPER as defined by EO 12333 and DoDM 5240.01. Such information should be handled and protected in accordance with applicable Intelligence Oversight rules by persons and organizations subject to those rules. DCSA collects, retains, and disseminates USPI in accordance with all applicable laws, directives, and policies. Should you require minimized USPI, contact Eric Kutchins, Commercial 571-305-6592, Eric.d.kutchins.civ@mail.mil.

(U) DCSA. 20 April 2021. “DCSA-SIB-0038-21: Likely Chinese APT using Pulse Secure VPN Vulnerability to Attack Cleared Contractors.”

(U) FireEye. 20 April 2021. “Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day.” https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

(U) CISA. 22 April 2021. “Analysis Report (AR21-112A): CISA Identifies SUPERNOVA Malware During Incident Response.” https://us-cert.cisa.gov/ncas/analysis-reports/ar21-112a

(U) CISA. 27 January 20201. “Malware Analysis Report (AR21-027A): MAR-10319053-1.v1 – Supernova.” https://us-cert.cisa.gov/ncas/analysis-reports/ar21-027a

(U) DCSA. 19-22 April 2021. Multiple Undisclosed Mandatory ICF Report Submissions.

(U) Pulse Secure. 20 April 2021. “KB44755 - Pulse Connect Secure (PCS) Integrity Assurance.” https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755

(U) Pulse Secure. 3 May 2021. “SA44784 - 2021-04: Out-of-Cycle Advisory: Multiple Vulnerabilities Resolved in Pulse Connect Secure 9.1R11.4."
https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784