Active Exploitation of Pulse Secure Zero-Day Vulnerabilities by Multiple Threat Actors

Executive Summary

VPN provider Ivanti Pulse Secure has released mitigations for multiple actively exploited vulnerabilities affecting the Pulse Connect Secure (PCS) SSL VPN appliance, including a new vulnerability tracked as CVE-2021-22893 Because multiple state-sponsored threat actors have been observed exploiting this vulnerability in the wild, the newly discovered vulnerability has been assigned the highest possible severity rating (10/10). Pulse Secure has released mitigations and plans to release a security update in early May. Although Pulse Secure has stated only a small number of customers were the subject of active exploitation of these vulnerabilities, both Pulse Secure and CISA recommend that customers use the recently released Ivanti Pulse Connect Secure Integrity Tool to determine if any systems are impacted. Currently, there is no evidence that these attacks have introduced any backdoors or supply chain compromise. While no Healthcare and Public Health (HPH) Sector entities have been publicly identified as victims, HPH organizations using PCS should act to mitigate these vulnerabilities.

Report

Reports from Ivanti Pulse Secure, FireEye, and CISA confirm that multiple threat actors have exploited vulnerabilities in the Pulse Connect Secure SSL VPN appliance to target government agencies, defense contractors, and critical infrastructure entities, among others. According to Pulse Secure, the vast majority of recent attacks against customers have exploited vulnerabilities discovered in 2019 and 2020: CVE-2019-11510, CVE-2020-8243, and CVE-2020-8260. However, threat actors have also targeted a small number of customers with the newly discovered and extremely severe CVE-2021-22893. This vulnerability allows for the execution of arbitrary code and placement of web shells on the PCS appliance that enables threat actor to bypass both standard and multi-factor authentication (MFA). Successful exploitation may persist through patching.

Mandiant is currently tracking 12 malware families associated with the exploitation of these vulnerabilities on Pulse Secure VPN devices, although the different malware families have been observed operating separately and are likely to be the work of multiple threat actors or groups working independently. Mandiant also identified several groups exploiting CVE-2021-22893, including UNC2630. This "uncategorized" (or UNC) group may be associated with APT 5 and is suspected to work on behalf of the Chinese government. Mandiant observed UNC2630 targeting U.S. defense companies as early as August 2020 through March 2021. Historically, this group has targeted American companies in the defense and technology sectors and the U.S. government.

Mitigations

Pulse Secure has released the "Workaround-2104.xml" file on their website as a mitigation for CVE-2021-22893. This XML file disables the Windows File Share Browser and Pulse Secure Collaboration features and uses a blacklist function to block URL-based attacks. However, "Workaround-2014.xml" will not work on PCS versions 9.0R1 - 9.0R4.1 or 9.1R1 - 9.1R2. If an organization's PCS is running one of these versions, it must be upgraded before importing the XML file. Pulse Secure also recommends that organizations using a PCS license server minimize the number of users that can connect to a server, placing the server on a management VLAN, or having a firewall enforce source-IP restrictions rather than using the Workaround-2104 mitigation.

Customers can use the Pulse Connect Secure Integrity Tool, available as "KB44755 - Pulse Connect Secure (PCS) Integrity Assurance" on their website, to determine if systems are impacted and identify any unusual system activity. A link to the Integrity Tool is included in the References section. CISA has released an alert (AA21-110A) advising PCS customers to immediately run the released Integrity Tool, update to the latest version of PCS, and investigate for malicious activity if necessary. If the Integrity Checker Tool identifies any mismatched or unauthorized files, CISA advises the following:

- Contact CISA to report your findings.
- Contact Ivanti Pulse Secure for assistance in capturing forensic information.
- Review "Unauthenticated Web Requests" log for evidence of exploitation, if enabled.
- Change all passwords associated with accounts passing through the Pulse Secure environment (including user accounts, service accounts, administrative accounts and any accounts that could be modified by any account described above, all of these accounts should be assumed to be compromised). Note: Unless an exhaustive password reset occurs, factory resetting a Pulse Connect Secure appliance will only remove malicious code from the device and may not remove the threat actor from the environment. Threat actors may use harvested credentials to regain access even after an appliance is fully patched.
- Review logs for any unauthorized authentications originating from the Pulse Connect Secure appliance IP address or the DHCP lease range of the Pulse Connect Secure appliance's VPN lease pool.
- Look for unauthorized applications and scheduled tasks in the network environment.
- Ensure no new administrators were created or non-privileged users were added to privileged groups.
- Remove any remote access programs not approved by the organization.
- Carefully inspect scheduled tasks for scripts or executables that may allow a threat actor to connect to an environment.

In a statement from Pulse Secure, the organization stated that the PCS team is in contact with a limited number of customers who have experienced evidence of exploit behavior on their PCS appliances. While the company stressed that they are aware of only a small number of impacted customers, Pulse Secure advised that affected organizations use a forensic provider to ensure a comprehensive investigation. Pulse Secure has released further recommendations, including installing available mitigations, password reset even if MFA is enabled, and reviewing the configuration to ensure no service accounts can be used to authenticate to the vulnerability. Security updates to solve this issue will be released in early May.

Analyst Comment

HC3 analysts assess with moderate confidence that the identified PCS vulnerabilities pose a risk to the HPH sector. While available reporting has identified the primary target as the U.S. defense industrial sector, the severity of CVE-2021-22893 combined with the lack of complete mitigations for the vulnerability and the prevalence of Pulse Secure usage increases the risk to the HPH sector.

MITRE ATT&CK Techniques

FireEye provided the following list of MITRE ATT&CK techniques used by malware they observed exploiting these vulnerabilities. Additional information about the identified MITRE ATT&CK techniques can be found in their report, linked in the References Section.

- T1003-OS Credential Dumping
- T1016-System Network Configuration Discovery
- T1021.001-Remote Desktop Protocol
- T1027-Obfuscated Files or Information
- T1036.005-Match Legitimate Name or Location
- T1048-Exfiltration Over Alternative Protocol
- T1049-System Network Connections Discovery
- T1053-Scheduled Task/Job
- T1057-Process Discovery

- T1059-Command and Scripting Interpreter
- T1059.003-Windows Command Shell
- T1070-Indicator Removal on Host
- T1070.001-Clear Windows Event Logs
- T1070.004-File Deletion
- T1071.001-Web Protocols
- T1082-System Information Discovery
- T1098-Account Manipulation
- T1105-Ingress Tool Transfer
- T1111-Two-Factor Authentication Interception
- T1133-External Remote Services
- T1134.001 Access Token Manipulation: Token Impersonation/Theft
- T1136-Create Account
- T1140-Deobfuscate/Decode Files or Information
- T1190-Exploit Public-Facing Application
- T1505.003-Web Shell
- T1518-Software Discovery
- T1554-Compromise Client Software Binary
- T1556.004-Network Device Authentication
- T1592.004 Gather Victim Host Information: Client Configurations
- T1562 Impair Defenses
- T1569.002-Service Execution
- T1574 Hijack Execution Flow
- T1600-Weaken Encryption

References

"Alert (AA21-110A): Exploitation of Pulse Connect Secure Vulnerabilities," CISA. April 20, 2021. https://us-cert.cisa.gov/ncas/alerts/aa21-110a

"Emergency Directive 21-03 April 20, 2021 Mitigate Pulse Secure Product Vulnerabilities," CISA. April 20, 2021. https://cyber.dhs.gov/ed/21-03/

Gatlan, Sergiu. "Pulse Secure VPN zero-day used to hack defense firms, govt orgs," Bleeping Computer. April 20, 2021. https://www.bleepingcomputer.com/news/security/pulse-secure-vpn-zero-day-used-to-hack-defense-firms-govt-orgs/

"KB44764 - Customer FAQ: PCS Security Integrity Tool Enhancements," Pulse Secure. April 16, 2021. https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44764/?l=en_US&fs=RelatedArticle

"KB44755 - Pulse Connect Secure (PCS) Integrity Assurance," Pulse Secure. April 19, 2021. https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755

"SA44101 - 2019-04: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.0RX," Pulse Secure. April 24, 2019. https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44101/

"SA44588 - 2020-09: Out-of-Cycle Advisory: Multiple vulnerabilities resolved in Pulse Connect Secure / Pulse Policy Secure 9.1R8.2," Pulse Secure. September 23, 2020. https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44588

"SA44601 - 2020-10: Security Bulletin: Multiple Vulnerabilities Resolved in Pulse Connect Secure / Pulse Policy Secure / Pulse Secure Desktop Client 9.1R9," Pulse Secure. October 26, 2020. https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44601

"SA44784 - 2021-04: Out-of-Cycle Advisory: Pulse Connect Secure RCE Vulnerability (CVE-2021-22893)," Pulse Secure. April 20, 2021. https://kb.pulsesecure.net/pkb_mobile#article/I:en_US/SA44784/s

Perez, Dan et al. "Check Your Pulse: Suspected APT Actors Leverage Authentication Bypass Techniques and Pulse Secure Zero-Day," FireEye. April 20, 2021. https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html