Exploitation of Pulse Connect Secure Vulnerabilities

Executive Summary
Since June 2020, unidentified threat actors have targeted vulnerabilities in certain Ivanti Pulse Connect Secure products. Threat actors gained initial access through the targeting of the following vulnerabilities: CVE-2019-11510, CVE-2020-8260, CVE-2020-8243, and CVE-2021-22893.

Upon exploitation, the threat actors “place webshells on the Pulse Connect Secure appliance for further access and persistence.” The threat actors’ access can allow them to perform: authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching.

Report
Alert (AA21-110A) Exploitation of Pulse Connect Secure Vulnerabilities
https://us-cert.cisa.gov/ncas/alerts/aa21-110a

Impact to HPH Sector
This vulnerability is continuing to affect organizations using Ivanti Pulse Connect Secure products within U.S. government agencies, critical infrastructure entities, and other private sector organizations. While the impact to the HPH Sector is currently unknown, the threat actors’ targeting of critical infrastructure leaves the HPH as a potential target. Please remain informed on updates to these vulnerabilities as new information is reported.

References
CISA – Samples of Malware Targeting Pulse Secure Devices

Pulse Secure – KB44755 - Pulse Connect Secure (PCS) Integrity Assurance Tool
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755

CISA – STIX-formatted list of indicators of compromise associated with the vulnerabilities

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

Contact Information
If you have any additional questions, please contact us at HC3@hhs.gov.