CyberSOC Threat Notification

Pulse Secure Connect RCE Vulnerability

Executive Summary

On April 20th, 2021, Mandiant disclosed that it had responded to compromises of Pulse Secure VPN appliances. These involved multiple techniques for bypassing single and multifactor authentication on Pulse Secure VPN devices, persisting across upgrades, and maintaining access through webshells.

Description

These compromises were due to exploitation of previously known vulnerabilities as well a previously unknown vulnerability, CVE-2021-22893, discovered in April 2021. These exploits were first investigated by Mandiant and occurred at organizations around the world. There are currently 12 known malware families associated with these exploits, which are related to the circumvention of authentication and backdoor access.

Affected Products

- Pulse Secure Connect VPN

Safeguards/Recommendations

Affected customers are strongly advised to utilize the most recent version of Pulse Connect Secure Integrity Tool to assess if systems have been impacted.

Resources

- https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html
- https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755
- https://github.com/fireeye/pulsesecure_exploitation_countermeasures/

Version History

Version 1. Initial Report

Vendor: Ivanti

CVE-ID: CVE-2021-22893

Published: APR 20, 2021

CVSS V3 Overall score: 10

Criticality: Critical

Patch Availability: Due May 2021

Vulnerability Type: Remote Code Execution

Exploitability Metrics

Attack Vector: Network

Attack Complexity: Low

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: Changed

Confidentiality: High

Integrity: High

Availability: High

Confidence Metrics

Exploitability: Proven

Remediation Level: Official Remediation

Report Confidence: Confirmed

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io