CYBERSECURITY ADVISORY

# Continued Exploitation of Pulse Secure VPN Vulnerability

**Last Revised:** April 15, 2020 **Alert Code:** AA20-010A

Give Feedback

## Summary

Unpatched Pulse Secure VPN servers continue to be an attractive target for malicious actors. Affected organizations that have not applied the software patch to fix an arbitrary file reading vulnerability, known as CVE-2019-11510, can become compromised in an attack.[1 <https://nvd.nist.gov/vuln/detail/cve-2019-11510>]

Although Pulse Secure [2] disclosed the vulnerability and provided software patches for the various affected products in April 2019, the Cybersecurity and Infrastructure Security Agency (CISA) continues to observe wide exploitation of CVE-2019-11510.[3

<https://www.kb.cert.org/vuls/id/927237/>],[4 <https://www.cisa.gov/news-events/alerts/2019/07/26/vulnerabilities-multiple-vpn-applications>],[5 <https://www.cisa.gov/news-events/alerts/2019/10/16/multiple-vulnerabilities-pulse-secure-vpn>]

CISA expects to see continued attacks exploiting unpatched Pulse Secure VPN environments and strongly urges users and administrators to upgrade to the corresponding fixes.[2]

## Timelines of Specific Events

- April 24, 2019 – Pulse Secure releases initial advisory and software updates addressing multiple vulnerabilities.
- May 28, 2019 – Large commercial vendors get reports of vulnerable VPN through HackerOne.
- July 31, 2019 – Full use of exploit demonstrated using the admin session hash to get complete shell.
- August 8, 2019 – Meh Chang and Orange Tsai demonstrate the VPN issues across multiple vendors (Pulse Secure) with detailed attack on active VPN exploitation.
- August 24, 2019 – Bad Packets identifies over 14,500 vulnerable VPN servers globally still unpatched and in need of an upgrade.
- October 7, 2019 – The National Security Agency (NSA) produces a Cybersecurity Advisory on Pulse Secure and other VPN products being targeted actively by advanced persistent threat actors.
- October 16, 2019 – The CERT Coordination Center (CERT/CC) releases Vulnerability Note VU#927237: Pulse Secure VPN contains multiple vulnerabilities.
- January 2020 – Media reports cybercriminals now targeting unpatched Pulse Secure VPN servers to install REvil (Sodinokibi) ransomware.

# Technical Details

## Impact

A remote, unauthenticated attacker may be able to compromise a vulnerable VPN server. The attacker may be able to gain access to all active users and their plain-text credentials. It may also be possible for the attacker to execute arbitrary commands on each VPN client as it successfully connects to the VPN server.

Affected versions:

- Pulse Connect Secure 9.0R1 - 9.0R3.3
- Pulse Connect Secure 8.3R1 - 8.3R7
- Pulse Connect Secure 8.2R1 - 8.2R12
- Pulse Connect Secure 8.1R1 - 8.1R15
- Pulse Policy Secure 9.0R1 - 9.0R3.1
- Pulse Policy Secure 5.4R1 - 5.4R7
- Pulse Policy Secure 5.3R1 - 5.3R12
- Pulse Policy Secure 5.2R1 - 5.2R12
- Pulse Policy Secure 5.1R1 - 5.1R15

Give Feedback

# Mitigations

This vulnerability has no viable workarounds except for applying the patches provided by the vendor and performing required system updates.

CISA strongly urges users and administrators to upgrade to the corresponding fixes.[2]

# References

[1] NIST NVD CVE-2019-11510 <https://nvd.nist.gov/vuln/detail/cve-2019-11510>

[2] Pulse Secure Advisory SA44101

[3] CERT/CC Vulnerability Note VU#927237 <https://www.kb.cert.org/vuls/id/927237/>

[4] Vulnerabilities in Multiple VPN Applications | CISA <https://www.cisa.gov/news-events/alerts/2019/07/26/vulnerabilities-multiple-vpn-applications>

[5] Multiple Vulnerabilities in Pulse Secure VPN | CISA <https://www.cisa.gov/news-events/alerts/2019/10/16/multiple-vulnerabilities-pulse-secure-vpn>

# Revisions

**January 10, 2020:** Initial Version

**April 15, 2020:** Revised to correct type of vulnerability.

Give Feedback

## Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

**News & Events** </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

**CISA Central**

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

USA.gov <https://www.usa.gov/>

Website Feedback </forms/feedback>

Give Feedback