LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY


# Pulse Secure VPN Servers Leak: Incident Case Study

**08/27/2020**

***Report #: 202008271030***

# Agenda

- Bottom Line Up Front: Patch
- What is XSS[.]is?
- Incident
- Identification of Exploited Vulnerability
- What is CVE-2019-11510?
- Timeline of CVE-2019-11510
- Severity
- Incident Takeaways

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

# BLUF: Patch CVE-2019-11510

If your organization uses Pulse Secure VPN, ensure that you have patched this vulnerability by updating to

- Version 8.2R12.1 or later
- Version 8.3R7.1 or later
- Version 9.0R3.4 or later

**Patches for this vulnerability were published in April 2019 and are available through the Pulse Secure Download Center at https://my.pulsesecure.net. There is no other mitigation for this vulnerability.**

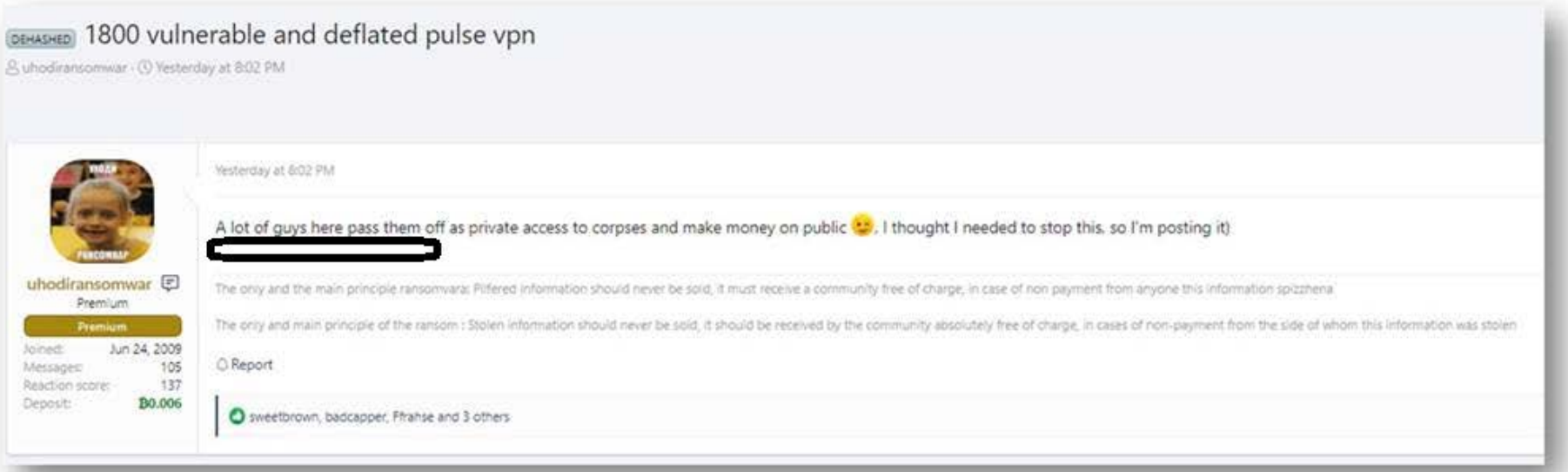
Once you have patched, change your organization's passwords to avoid threat actors abusing already-leaked credentials.

# XSS[.]is Forum

- XSS – Cross Site Scripting
- Cybercriminal forum
- Relaunched in 2018 based on now-defunct “DamageLab” forum
- Experienced team of administrators
- Commonwealth of Independent States-affiliated
- Over 19k members and 162k posts in November 2019
- Frequented by prominent Russian-affiliated cybercriminals
  - Ransomware gangs REvil (Sodinokibi), NetWalker, Lockbit, Avaddon, Makop, and Exorcist have threads on the forum and openly recruit members and customers


*Source: Digital Shadows*

# Discovered August 4, 2020 on XSS



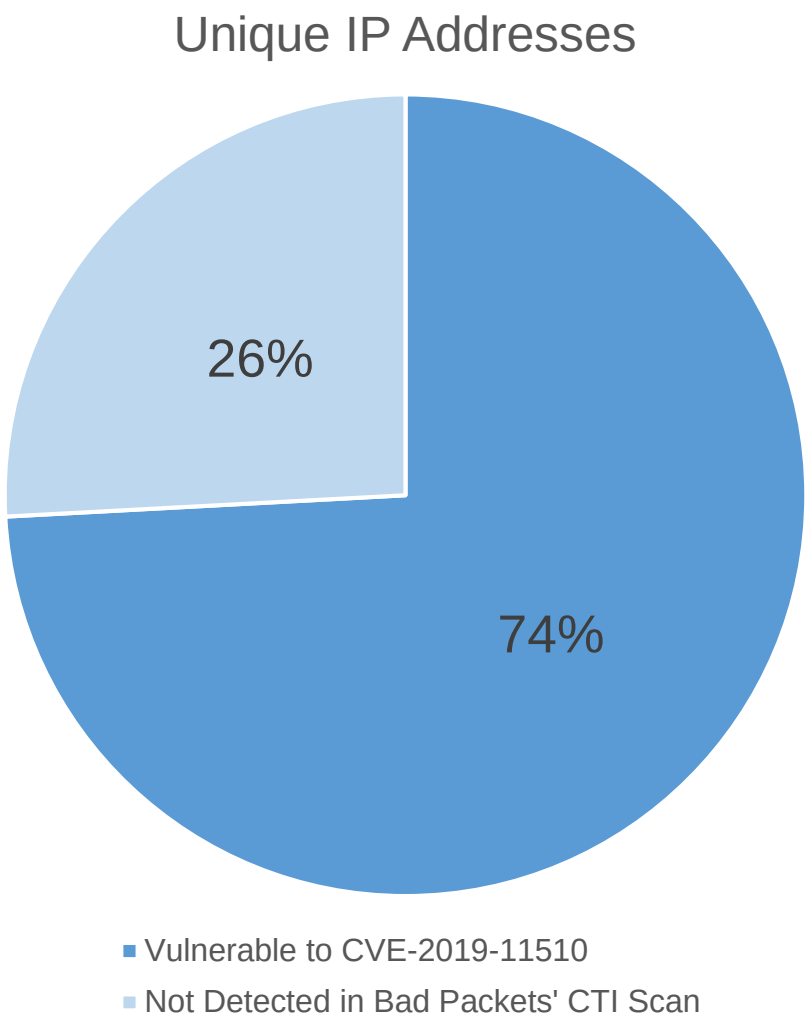

*Source: ZDNet*

The post above advertised 1800 vulnerable servers but reporters at ZDNet found only 913. The list included the following information for each server:

- Pulse Secure VPN server firmware version
- SSH server keys for each exposed server
- All local users and password hashes
- Administrator account details
- Any previous VPN logins, **including plaintext credentials**
- Session cookies

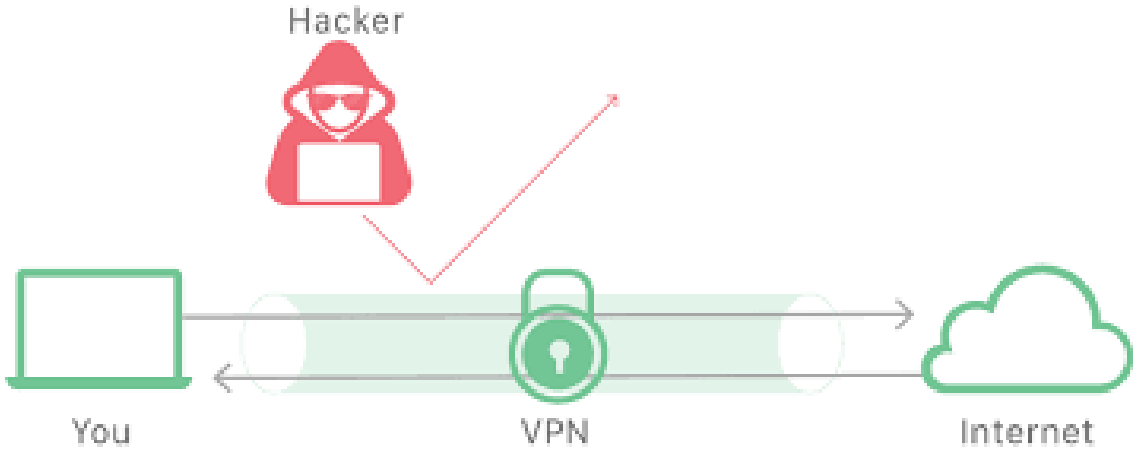
# Unpatched Vulnerability Left Organizations Open to Exploitation

- Cyber threat intelligence firm Bad Packets reported: “of the 913 unique IP addresses found in that dump, 677 were detected . . . to be vulnerable to **CVE-2019-11510** when the exploit was made public last year.”
- The remaining 26% of IP addresses may also be vulnerable
- Threat intelligence analyst “Bank Security” suggested that the hacker who compiled this list scanned the entire internet IPv4 address space for Pulse Secure VPN servers, used an exploit for the CVE-2019-11510 vulnerability to gain access to systems, and then collected all the information in one central repository.



# Threat Actors likely exploited CVE-2019-11510

- CVE-2019-11510: “Unauthenticated remote attacker with network access via HTTPS can send a specially crafted Uniform Resource Identifier (URI) to perform an arbitrary file reading vulnerability” – NIST’s National Vulnerability Database
  - A malicious URI (such as an URL) can pass and run arguments, parameters and data to an external application
- The flaw could allow a remote, unauthenticated attacker to obtain usernames and plaintext passwords from vulnerable endpoints.
- Once usernames, passwords, and other information is recorded, an attacker has full access to all information, data, and programs maintained within the VPN
  - Many organizations use VPNs to restrict access to sensitive data and programs




*Source: Cloudflare*

# Timeline of CVE-2019-11510

| | |
|---|---|
| 22MAR19 | • Security researchers disclose vulnerability to Pulse Secure |
| 24APR19 | • Pulse Secure provides a patch fix, states vulnerability is “highly critical,” begins contacting customers directly to encourage patching |
| 24AUG19 | • Security researchers identify 14,500 vulnerable VPN servers globally still unpatched and in need of an upgrade |
| 7OCT19: | • NSA produces a Cybersecurity Advisory on Pulse Secure and other VPN products being targeted actively by Advanced Persistent Threat (APT) actors |
| 2JAN20: | • Company running seven unpatched Pulse Secure VPN servers has website taken offline in Sodinokibi (REvil) ransomware attack |
| 3JAN20 | • At least 3,825 Pulse Secure VPN servers, including more than 1,300 located in the U.S., remain unpatched and vulnerable |
| 24JUN20 – 8JUL20: | • Entire internet IPv4 address space for Pulse Secure VPN servers scanned and list compiled by threat actor |
| 4AUG20 | • List posted on XSS[.]is by uhodiransomwar |
| 5AUG20: | • Another threat actor published list of domains – including government and banking domains – related to posted IPs |

# “A Literal DEFCON 1”

- **“The publication of this list as a free download is a literal DEFCON 1 danger level for any company that has failed to patch its Pulse Secure VPN over the past year” – ZDNet**
- Assume ransomware gangs are actively exploiting this list
- Organizations cannot assume that this is the full list of potential victims
- Organizations using other VPNs that are affected by similar vulnerabilities should also patch

# Incident Takeaways

- **Prioritize patching critical vulnerabilities with active exploits**
- VPNs are attractive targets
- Advanced Persistent Threats (APTs) actively target organizations through VPNs
  - Deploy malware, including ransomware
  - Steal intellectual property
  - Monitor traffic and gather intelligence
- Healthcare and Public Health organizations involved in COVID research at particular risk
- Even when companies release patches, customers may not update or patch
- Vulnerabilities in Pulse Secure, Palo Alto, and Fortinet VPNs are being actively exploited

# Reference Materials

# References


- ZDNet, Hacker leaks passwords for 900+ enterprise VPN servers
  - https://www.zdnet.com/article/hacker-leaks-passwords-for-900-enterprise-vpn-servers/
- Digital Shadows, Forums Are Forever – Part 1: Cybercrime Never Dies
  - https://www.digitalshadows.com/blog-and-research/forums-are-forever-part-1-cybercrime-never-dies/
- Common Vulnerabilities and Exposures, CVE-2019-11510
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11510
- CERT Coordination Center, Pulse Secure VPN contains multiple vulnerabilities
  - https://www.kb.cert.org/vuls/id/927237/
- SCMagazine, Thousands of businesses at risk via Pulse Secure VPN flaw (updated with response)
  - https://www.scmagazineuk.com/thousands-businesses-risk-via-pulse-secure-vpn-flaw-updated-response/article/1670064
- Tenable, CVE-2019-11510: Critical Pulse Connect Secure Vulnerability Used in Sodinokibi Ransomware Attacks
  - https://www.tenable.com/blog/cve-2019-11510-critical-pulse-connect-secure-vulnerability-used-in-sodinokibi-ransomware
- TechTarget, Preparing for uniform resource identifier (URI) exploits
  - https://searchsecurity.techtarget.com/tip/Preparing-for-uniform-resource-identifier-URI-exploits
- ZDNet, A Chinese APT is now going after Pulse Secure and Fortinet VPN servers
  - https://www.zdnet.com/article/a-chinese-apt-is-now-going-after-pulse-secure-and-fortinet-vpn-servers/

# Questions

# Questions

## Upcoming Briefs

- CIS 20 Controls and HPH (9/3)
- File-less Malware (9/10)

## *Requests for Information*

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

## *Product Evaluations*

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.


HC3 Customer Feedback

## *Disclaimer*

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

# About Us

*HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector*

## Products

### Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

### White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

### Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

# Contact


www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV