CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-021

Critical Vulnerability in Pulse Connect Secure

August 5, 2021 — v1.4

TLP:WHITE

History:

- 21/04/2021 — v1.0 – Initial publication
- 03/05/2021 — v1.1 – Update about new PCS release (9.1R11.4)
- 17/05/2021 — v1.2 – Update about newly discovered vulnerability
- 14/06/2021 — v1.3 – Update about new PCS release (9.1R11.5)
- 05/08/2021 — v1.4 – Update about new PCS release (9.1R12)

Summary

On April 20, 2021, Ivanti has announced that a vulnerability (CVE-2021-22893) was discovered in their Pulse Connect Secure (PCS) product. While initially a patch was not available, the vendor released information on how to mitigate the vulnerability. Furthermore, on 3 May 2021, Ivanti has released PCS version 9.1R11.4, which fixes the initially identified vulnerability along with three others [1, 2]. Three of the identified vulnerabilities have a **critical CVSS score**, the first of which has been observed to be exploited in the wild. These vulnerabilities pose significant risks and have been widely reported on [4, 5, 6, 7].

On May 14, 2021, Ivanti has released another security advisory addressing yet another vulnerability (CVE-2021-22908) also affecting the recently released version 9.1R11.4 which fixes the aforementioned ones [8]. The newly discovered vulnerability is a *buffer overflow* with a CVSS score of 8.5. At the time the vendor provided mitigation measures to apply until the vulnerability is patched.

On June 11, 2021, PCS version 9.1R11.5 was released [9], which provides the security hardening required to patch this latest vulnerability.

On August 5, 2021, Ivanti has published another security advisory [10] addressing multiple vulnerabilities affecting Pulse Connect Secure versions prior to 9.1R12. This last release fixes all vulnerabilities and also includes enhanced features such as the incorporation of the Pulse Security Integrity Checker Tool directly into the product.

Technical Details

Vulnerabilities patched on 3rd of May, 2021 in PCS version 9.1R11.4 [1]:

- **CVE-2021-22893** *(CVSS Score 10.0)* - Multiple use after free in Pulse Connect Secure before 9.1R11.4 allows a remote unauthenticated attacker to execute arbitrary code via license services.
- **CVE-2021-22894** *(CVSS Score 9.9)* - Buffer overflow in Pulse Connect Secure Collaboration Suite before 9.1R11.4 allows a remote authenticated users to execute arbitrary code as the root user via maliciously crafted meeting room.
- **CVE-2021-22899** *(CVSS Score 9.9)* - Command Injection in Pulse Connect Secure before 9.1R11.4 allows a remote authenticated users to perform remote code execution via Windows File Resource Profiles.
- **CVE-2021-22900** *(CVSS Score 7.2)* - Multiple unrestricted uploads in Pulse Connect Secure before 9.1R11.4 allow an authenticated administrator to perform a file write via a maliciously crafted archive upload in the administrator web interface.

Vulnerabilities reported on 14 May 2021 - patched on 11th of June, 2021 in PCS version 9.1R11.5 [8, 9]:

- **CVE-2021-22908** - *(CVSS Score 8.5)* - Buffer Overflow in Windows File Resource Profiles in 9.X allows a remote authenticated user with privileges to browse SMB shares to execute arbitrary code as the root user. As of version 9.1R3, this permission is not enabled by default.

Vulnerabilities reported on 5 August 2021 - patched on 2nd of August, 2021 in PCS version 9.1R12 [10]:

- **CVE-2021-22937** *(CVSS Score 9.1)* - A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform a file write via a maliciously crafted archive uploaded in the administrator web interface.
- **CVE-2021-22933** *(CVSS Score 7.6)* - A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform an arbitrary file delete via a maliciously crafted web request.
- **CVE-2021-22934** *(CVSS Score 8.0)* - A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator or compromised Pulse Connect Secure device in a load-balanced configuration to perform a buffer overflow via a malicious crafted web request.
- **CVE-2021-22935** *(CVSS Score 9.1)* - A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform command injection via an unsanitized web parameter.
- **CVE-2021-22936** *(CVSS Score 8.2)* - A vulnerability in Pulse Connect Secure before 9.1R12 could allow a threat actor to perform a cross-site script attack against an authenticated administrator via an unsanitized web parameter.
- **CVE-2021-22938** *(CVSS Score 7.9)* - A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform command injection via an unsanitized web parameter in the administrator web console.

Detection

Access to the following URLs may facilitate the exploitation of some vulnerabilities [1]:

```
^/+dana/+meeting
^/+dana/+fb/+smb
^/+dana-cached/+fb/+smb
^/+dana-ws/+namedusers
^/+dana-ws/+metric
```

Investigation of past and current logs may help identify potential exploitation attempts. Access to these URLs should be blocked once the mitigations described below are applied.

Products Affected

- By CVE-2021-22893 - PCS 9.0R3/9.1R1 up to PCS 9.1R11.3
- By CVE-2021-22894, CVE-2021-22899, CVE-2021-22900 - PCS 9.1Rx and 9.0Rx up to PCS 9.1R11.3
- By CVE-2021-22908 - PCS 9.0RX and 9.1RX up to 9.1R11.4
- By CVE-2021-22937, CVE-2021-22933, CVE-2021-22934, CVE-2021-22935, CVE-2021-22936, CVE-2021-22938 - PCS before 9.1R12

Recommendations

The vulnerabilities listed above have been included in the latest version of PCS, 9.1R12, which was released on 2 August 2021 [10]. We strongly encourage you to upgrade to ensure your organization is protected.

The vendor has released an Integrity Tool [3], which allows to verify if the PCS device might have been compromised. It is important to note that the tool should be able to detect infections related to this new vulnerability as well as any previous infections that may have remained undetected. **It is hence strongly recommended to use this tool, on a very regular basis, to ensure the integrity of the PCS**. However, please note that running the tool will require a reboot. In case the Integrity Tool finds mismatched files or newly detected files, please download the *Admin Generated Snapshot* post-reboot and create a *Support Ticket* with Ivanti for further investigation [3]. In the latest version (9.1R12), the Pulse Security Integrity Checker Tool is directly built into the product. This built-in feature eliminates the need for scheduled downtime to run an integrity check [10].

Mitigations

While patches are available, the vendor also provided mitigation measures that prevent exploitation of these vulnerabilities. They can be mitigated by importing the `Workaround-2104.xml` file as described in [1] and `Workaround-2105.xml`. Furthermore, customers should disable the Windows File Browser - also as described in [1].

Please note that while PCS version 9.1R11.4 does not fully protect currently against the exploitation of CVE-2021-22908 and require deploying `Workaround-2105.xml`. PCS version 9.1R11.3 with applied mitigation `Workaround-2104.xml` also protects against CVE-2021-22908. In this case, deploying `Workaround-2105.xml` is not needed [8]. PCS version 9.1R11.5 fully protects against the known vulnerabilities.

References

[1] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44784

[2] https://blog.pulsesecure.net/pulse-connect-secure-security-update/

[3] https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44755

[4] https://www.fireeye.com/blog/threat-research/2021/04/suspected-apt-actors-leverage-bypass-techniques-pulse-secure-zero-day.html

[5] https://www.reuters.com/technology/china-linked-hackers-used-pulse-secure-flaw-target-us-defense-industry-2021-04-20/

[6] https://www.bleepingcomputer.com/news/security/pulse-secure-vpn-zero-day-used-to-hack-defense-firms-govt-orgs/

[7] https://www.cyberscoop.com/pulse-secure-china-exploit-mandiant/

[8] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44800

[9] https://www-prev.pulsesecure.net/download/techpubs/current/2373/pulse-connect-secure/pcs/9.1rx/9.1r11/ps-pcs-sa-9.1r11.5-releasenotes.pdf

[10] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/