CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-023

Pulse Connect Secure Severe Vulnerabilities

April 23, 2020 — v1.0

TLP:WHITE

History:

- *23/04/2020 — v1.0 – Initial publication*

Summary

On April 6, 2020, three issues were discovered in Host Checker policy enforcement on Pulse Secure Pulse Connect Secure (PCS). These vulnerabilities were encoded as CVE-2020-11580 (*No certificate Validation*) [1], CVE-2020-11581 (*Command Injection*) [2], CVE-2020-11582 (*DNS Rebindig*) [3]. These vulnerabilities could allow a man-in-the-middle (MITM) attacker to perform a remote code execution (RCE) attack.

CERT-EU is not aware of any malicious exploitation for those vulnerabilities, but we have to take into consideration that the file on which these vulnerabilities are built (`tncc.jar`) is not obfuscated in any way and the original source code can be obtained with almost any Java decompiler and customized in a malicious manner.

Technical Details

The Host Checker is a client side component that the Pulse Connect Secure appliance may require in order to connect to the VPN. The Host Checker requests a policy from the server and perform basic checks on the client accordingly. Checks may include MAC Addresses, running process (i.e., checking for an antivirus) and some others. While on Windows, the plugin is an ActiveX component, in Linux, Solaris and OSX it is a Java Applet [4].

An attacker who is in a position where he/she can perform a man-in-the-middle attack may spoof the server and send a malicious cookie along with a policy that is impossible to comply with. An example cookie could be any method of command injection on Linux. The client will then fail to comply with the policy and execute the command with the appended value when trying to show remediation instructions.

All the vulnerabilities are based on the applet in `tncc.jar`, executed on macOS, Linux, and Solaris clients when a Host Checker policy is enforced. In this case, three things can happen:

1. It accepts an arbitrary SSL certificate (CVE-2020-11580).

2. It allows a man-in-the-middle attacker to perform OS command injection attacks (against a client) via shell meta-characters to the `doCustomRemediateInstructions` method, because `Runtime.getRuntime().exec()` is used (CVE-2020-11581).
3. It launches a TCP server that accepts local connections on a random port that can be reached by local HTTP clients, because up to 25 invalid lines are ignored, and DNS re-binding can occur (CVE-2020-11582).

Products Affected

- All the existing versions of Pulse Connect Secure and Pulse Policy Secure as **servers**.
- For the clients, this issue is reported only on macOS, Linux and Solaris clients regardless of the installed version.
- Agent-less Host Checker uses an applet to send information to the PCS appliance. To launch the Host Checker Applet, Browsers should support NPAPI support (technology required for Java applets). As of September, 2018, Firefox, Chrome and Safari Browsers no longer offers a version which supports NPAPI. Firefox version 52ESR is the last release to support the technology.

Recommendations

A patch for these vulnerabilities has not been released yet, but some workarounds can be put in place in order to mitigate them:

- Safari 12 and above no longer supports NPAPI. If you are using older version, please upgrade your browsers to latest version.
- Google's Chrome version 45 and above have dropped support for NPAPI, and therefore Java Plugin do not work on these browsers anymore.
- Firefox no longer offers a version which supports NPAPI. Firefox version 52ESR is the last release to support the technology. If end users are using 52ESR, please recommend to upgrade the browser to latest version or use Pulse Secure Client.
- If Host Checker is not enabled on the PCS Appliance, end-users are not vulnerable to CVE-2020-11580, CVE-2020-11581, and CVE-2020-11582 [5].

References

[1] https://nvd.nist.gov/vuln/detail/CVE-2020-11580

[2] https://nvd.nist.gov/vuln/detail/CVE-2020-11581

[3] https://nvd.nist.gov/vuln/detail/CVE-2020-11582

[4] https://git.lsd.cat/g/pulse-host-checker-rce

[5] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44426