CVE-2019-11510

Arbitrary file reading vulnerability in Pulse Connect Secure

Martin Pretz, 7060026

May 10, 2021

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Proin a convallis magna. Etiam ac placerat metus, aliquam luctus orci. Integer maximus semper augue sit amet pulvinar. Etiam congue dolor quis arcu molestie, non sagittis quam porttitor. Etiam id sagittis justo, in eleifend leo. Maecenas dapibus nunc posuere venenatis pellentesque. Ut imperdiet dapibus magna, eu tincidunt nulla venenatis in. Cras consectetur quis diam id aliquam. Nulla id ante suscipit tellus tristique fermentum eu malesuada lectus. Sed mattis sem ut leo accumsan, quis sagittis purus cursus. Sed faucibus in dui id euismod. Curabitur pharetra porttitor risus sed luctus. Praesent nec augue turpis. Suspendisse maximus pretium eros, quis varius leo lobortis eget. Aliquam mollis id nibh at porttitor. Pellentesque sit amet magna auctor, dictum nisl ac, blandit ante. **population:online**

1 Introduction

2 Theoretical Foundations

2.1 SSL-VPN

Um die vorliegende Sicherheitslücke besser zu verstehen und einordnen zu können, muss zunächst geklärt werden was überhaupt SSL-VPN ist und wie es funktioniert.

In erster Linie handelt es sich bei eiem SSL-VPN um ein normales VPN welches in zweiter Linie um SSL ergänzt wird.

2.2 Pulse Connect Secure

3 Description of the Vulnerability

The CVE-2019-11510 is a critical vulnerability that allows attackers to get arbitrary file reading access after they have send a special URI.[1]
This vulnarability is part of the CWE-22 class which is associated with "Path Traversal". That means that by explicitly specifying an abnormal path that is "[...] intended to identify a file or directory [...]" [2] it is possible to gain access to that file or directory without owning the required rights. This is made possible because the software uses an externally specified path and due to the way the software proceeds with that path. The effect is that the software resolves the given paths to files or folders that lie outside the resitriced directory.[2]

4 Path traversal

Allthough path traversal was already mentioned in the previous chapter, one must take a closer look at path traversal in order to fully understand how it works and how it can be avoided. This will be done during the course of this chapter.

5 How can this vulnarability be exploited?

As already mentioned in 3, in order to exploit the vulnerability the attacker must send a request (e.g. via HTTP) to the target server that contains a path sequence used for path traversal (see chapter 4) and a special URI for the file that the attacker want to gain access to.[3]
"When a user logs into the admin interface of the VPN [...]"[3], the password is stored as plain-text within a MDB file (Microsoft Access Database). The corresponding file can be found at */data/runtime/mtmp/lmdb/dataa/data.mdb*. Since the attacker already has arbitrary access to all files of the system he can easyly obtain the admin password. With this information the attacker could perform further attacks, e.g. exploiting the CVE-2019-11508, which allows an attacker to upload harmful files while using the credentials he obtained since the credentials actually belong to an authanticated user.[3]

6 Example usage

7 Affected

All versions from between 8.2 to 8.2R12.1, 8.3 to 8.3R7.1 and 9.0 to 9.0R3.4 are affected.[1]

8 Solution

Since this vulnerability is caused by the unintended behaviour of Pulse Connect Secure while resolving provided paths and therefore the internal implementation of this software, the vulnerability has been removed by a software patch provided by Pulse Secure.

9 Conclusion

References

[1] *Nvd - cve-2019-11510*, https://nvd.nist.gov/vuln/detail/CVE-2019-11510, (Accessed on 05/10/2021).

[2] *Cwe - cwe-22: Improper limitation of a pathname to a restricted directory ('path traversal') (4.4)*, http://cwe.mitre.org/data/definitions/22.html, (Accessed on 05/10/2021).

[3] *Cve-2019-11510: Proof of concept available for arbitrary file disclosure in pulse connect secure - blog — tenable*, https://de.tenable.com/blog/cve-2019-11510-proof-of-concept-available-for-arbitrary-file-disclosure-in-pulse-connect-secure, (Accessed on 05/10/2021).