DefenseCode

PureVPN Windows Privilege Escalation Vulnerability

PureVPN Windows Privilege Escalation Vulnerability	
Advisory ID:	**DC-2018-02-001**
Software:	**PureVPN**
Version	**5.19.4.0 (Windows Build Version: 6)**
Vendor Status:	**Vendor contacted / Fixed**
Release Date:	**21/02/2018**
Risk:	**MEDIUM**

1. General Overview

During the security analysis of PureVPN's Windows client software it has been discovered that the software contains a vulnerability that could allow a local user to escalate their privileges on the system.

2. Software Overview

PureVPN is a paid VPN service provider which claims to provide online privacy and security to its users. The product is equipped with different tunneling protocols to offer end-to-end encryption to its users. PureVPN's network of 550+ servers is spread across more than 145 countries, serving over 1 million users from all over the world.

PureVPN provides client software for Windows, Mac, Android, and iOS.

Homepage:

https://www.purevpn.com

3. Vulnerability Description

During the security analysis of PureVPN Windows client software it has been determined that the software installation grants Everyone group (i.e all users) full control permission to the software's installation directory (*C:|Program Files (x86)|PureVPN* by default).

In addition, it has been determined that the *PureVPNService.exe*, which runs under NT Authority\SYSTEM privileges, tries to load several dynamic-link libraries using relative paths instead of the absolute path. When not using a fully qualified path, the application will first try to load the library from a directory from which the application is started. As the residing directory of *PureVPNService.exe* is writable to all users, this makes the application susceptible to privilege escalation through DLL hijacking.

DLL hijacking proof of concept was done by placing a malicious *cryptbase.dll* inside the software's installation directory, resulting in privilege escalation to NT Authority\SYSTEM when the PureVPNService.exe service is started.

4. Solution

Vendor fixed the reported security issues and released a new version. All users are strongly advised to update to the latest available version.

5. Credits

Discovered by Bosko Stankovic (bosko@defensecode.com).

6. Disclosure Timeline

02/02/2018	**Vendor contacted**
13/02/2018	**Vendor responded**
20/02/2018	**Vulnerability fixed**

7. About DefenseCode

DefenseCode L.L.C. delivers products and services designed to analyze and test web, desktop and mobile applications for security vulnerabilities.

DefenseCode ThunderScan is a SAST (Static Application Security Testing, WhiteBox Testing) solution for performing extensive security audits of application source code. ThunderScan performs fast and accurate analyses of large and complex source code projects delivering precise results and low false positive rate.

DefenseCode WebScanner is a DAST (Dynamic Application Security Testing, BlackBox Testing) solution for comprehensive security audits of active web applications. WebScanner will test a website's security by carrying out a large number of attacks using the most advanced techniques, just as a real attacker would.

Subscribe for free software trial on our website http://www.defensecode.com

E-mail: defensecode[at]defensecode.com

Website: http://www.defensecode.com
Twitter: https://twitter.com/DefenseCode/