Array Networks Security Advisory:
Session Cookie Exposure Vulnerability (CVE-2019-1573)

Advisory Date: April 24, 2019

Overview

GlobalProtect Agent 4.1.0 for Windows and GlobalProtect Agent 4.1.10 and earlier for MacOS may allow an attacker to access authentication and/or session tokens and replay them to spoof the VPN session and gain access as the user.
Reference: CVE-2019-1573 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1573

Impact

Array Networks' MotionPro Windows, MacOS, Linux, Android and iOS clients and Web-launched Array Client are affected by this vulnerability since session cookies are stored in plain text in the client log messages.

Solution

For MotionPro Windows, MacOS, Linux, Android and iOS clients, new versions will be released to address this vulnerability.
The solution will be available from the following MotionPro client versions at the end of April 2019:

- MotionPro Windows 1.2.3 release
- MotionPro MacOS 1.2.4 release
- MotionPro Linux 1.2.3 release
- MotionPro Android 3.0.7 release
- MotionPro Plus iOS 2.0.8 release

For the Web-launched Array Client with the ActiveX or Java component, please use the new MotionPro client instead.

1371 McCarthy Blvd. Milpitas, CA 95035 | Phone: (408) 240-8700 Toll Free: 1-866-MY-ARRAY | www.arraynetworks.com