INF-2022-11-03 - OpenSSL vulnerabilities & VPN Client

Overview

As a result of the recent information about the OpenSSL vulnerabilities, we have investigated all parts of the IXON Cloud, the IXrouter and the VPN Client. Luckily, except one part -which is not exploitable (detailed below)-, no part used the affected OpenSSL versions and therefore do not contain any risk for you or your environment.

The one part where we do use the affected OpenSSL version is in a specific part of the VPN Client, namely the implementation of stunnel (AKA stealth mode). This stealth mode is used to hide (re-encrypt) your VPN traffic for areas that restrict VPN usage. Due to the nature of our stunnel implementation, it is not possible to exploit the e-mail address overflow detailed in CVE-2022-3786 and CVE-2022-3602. Nevertheless, to avoid any confusion, we will release a new VPN Client (version 1.4.2) in the coming days which bundles the latest stunnel version which uses the patched OpenSSL 3.0.7.

Recommendations

No further action is needed from customers.

Additional information

https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/