April 11, 2014

Scopia Solution – OpenSSL Heartbleed Bug

As announced April 7, 2014, releases 1.0.1 through 1.0.1f of the popular Security Component "OpenSSL" has a flaw that allows an attacker to read large portions of private memory. This memory has been shown to include passwords and private keys associated with PKI certificates. The exploit leaves no traces that private information has been leaked. It is a very serious flaw, but only affects the most recent releases of OpenSSL. See http://www.kb.cert.org/vuls/id/720951

The only products effected by the above vulnerability are the XT endpoints (5000, 4200, XTE240) running the new 8.3 GA software released on March 27th 2014 – for these products we already have a new version in place (8.3.0.66) that was recompiled without the HEARTBEATS option according to the OpenSSL recommendation. The hotfix for the XT endpoints will be available early next week as a software upgrade.

We have identified all the products in the Scopia product line that are using the OpenSSL software package and none of them is running the relevant software version, as detailed in the table below

Product	OpenSSL version	Comments
Scopia Desktop Server	√	
Scopia Desktop Client	√	Mac & Windows
Scopia Mobile Client	√	iOS and Android
Scopia Elite MCU 6000	√	
Scopia Management	√	
Scopia Video Gateway for MS lync	√	
Scopia SIP Gateway	√	
Scopia TIP Gateway	√	
Scopia XT 1200	√	
Scopia XT 5000,4200,XTE240	√	For all version before 8.3
Scopia XT 5000,4200,XTE240	×	For 8.3 GA

All the other Scopia products that are not mentioned in this table do not have OpenSSL as part of their code.

© 2014 Avaya Inc.
All rights reserved. Avaya, Avaya Scopia and The Power of We are trademarks owned by Avaya Inc. Users are not permitted to use such trademarks without prior written consent from Avaya Inc.