GANZ gSOAP Statement

8-29-17 v1.0.0

Overview

Genivia's gSOAP Toolkit, which many video surveillance manufacturers implement in ONVIF, is known to have a vulnerability in its versions 2.7 to 2.8.47. The vulnerability is also known as the "Devil's Ivy." In this report, GANZ investigated what the vulnerability is, and whether or not GANZ PixelPro, PixelPro GXi, or GENSTAR IP cameras and encoders would be affected.

The determination is that these products are not affected.

gSOAP Vulnerability

Presently, most manufacturers use gSOAP to implement the ONVIF protocol.

In order to take advantage of the vulnerability, the attack would have to be configured separately for each vulnerable device or application, and requires sending two full gigabytes of data to a target. This is considered an unreasonably large amount of bandwidth. For current embedded devices, the largest memory size is 1GB. Since they are unable to accept the 2GB size of network data, this attack can't influence most embedded devices.

Risk Analysis

GANZ PixelPro and PixelPro GXi:

IP cameras and encoders filter XML data prior to forwarding to gSOAP to process ONVIF commands. All data from the external world is fed first to the web server. It is then handled by the gSOAP library after filtering of the data. The maximum data size the web server allows is less than 2GB. Due to this limitation, XML messages over 2GB would never reach the gSOAP library, and would instead display an HTTP error message.

GANZ GENSTAR:

IP cameras' current use of ONVIF utilizes the third-party tool gSOAP, but the ONVIF implementation does not provide direct access to services. Functions are achieved by internally packaged services for protection purposes, which disallows access for a direct outside attack. The external ONVIF services encapsulate to add security restrictions, and the maximum data accepted is 30K. If the data is over 30K, it will be discarded.

RECOMMENDATIONS

Considering the characteristics of the network monitoring equipment, we encourage users to strengthen their own network monitoring through network security means, such as installation of firewalls to detect and block network attacks.

Conclusion

The known vulnerability mentioned in the advisory notice from Genivia does not affect GANZ PixelPro, PixelPro GXi, or Genstar network devices, and the advisory relating to the flaw of gSOAP is not relevant to our equipment. Therefore, no action is necessary for customers who use these GANZ IP cameras and encoders.

