Hanwha Techwin

gSOAP 보안 취약점 관련 당사 영향도 분석 및 공지

[배경]

1. AXIS에서 발생한 gSOAP 관련 보안 취약점이 ONVIF 기술서비스 위원회에게 공유가 되었으며, ONIVF 회원사(당사 포함)들에게 gSOAP 내에 포함된 보안 취약점에 대해 패치할 것을 공지하였습니다. (6/27)

   * gSOAP은 Onvif의 SOAP 프로토콜을 Genivia社가 구현한 오픈소스/상용(듀얼) 라이선스 SW임

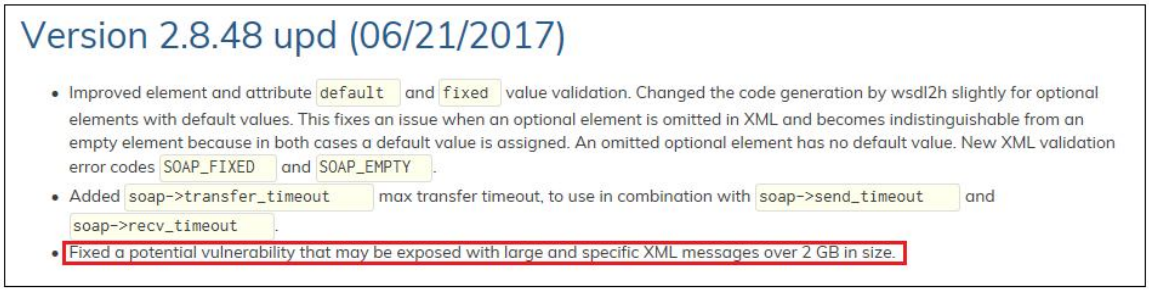
2. 해당 보안 취약점에 대해 AXIS社는 자체 Security Advisory를 발행(7/11)하였으며 CVE 사이트에는 아직 공개가 되어 있지는 않습니다(CVE-2017-9765 ID만 부여된 상태).

   * Genivia社는 해당 보안 취약점을 패치한 버전(2.8.48)을 기 배포하였습니다. (6/21)

     https://www.genivia.com/changelog.html

     https://www.genivia.com/advisory.html

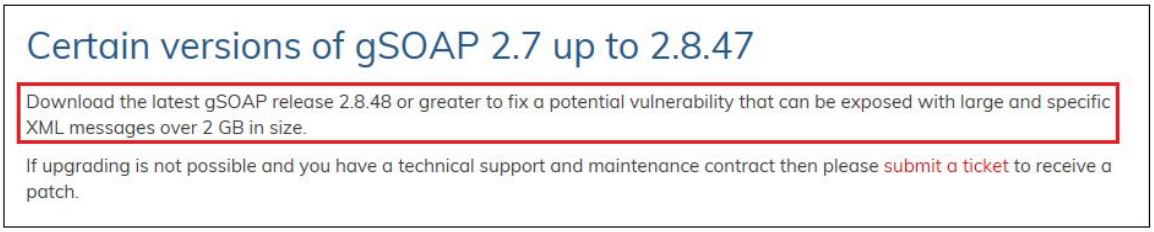
   * 해당 취약점은 SOAP Webservices 데몬에서 사용하는 XML 메시지의 Stack Buffer Overflow 공격을 통해 기기의 사용자 권한을 탈취하는데 악용될 수 있습니다.



Version 2.8.48 upd (06/21/2017)

- Improved element and attribute `default` and `fixed` value validation. Changed the code generation by wsdl2h slightly for optional elements with default values. This fixes an issue when an optional element is omitted in XML and becomes indistinguishable from an empty element because in both cases a default value is assigned. An omitted optional element has no default value. New XML validation error codes `SOAP_FIXED` and `SOAP_EMPTY`.
- Added `soap->transfer_timeout` max transfer timeout, to use in combination with `soap->send_timeout` and `soap->recv_timeout`.
- Fixed a potential vulnerability that may be exposed with large and specific XML messages over 2 GB in size.

   * 하기의 2.8.47은 2.8.48의 오타로 보이며, 내용은 2.8.48로 되어 있습니다.



Certain versions of gSOAP 2.7 up to 2.8.47

Download the latest gSOAP release 2.8.48 or greater to fix a potential vulnerability that can be exposed with large and specific XML messages over 2 GB in size.

If upgrading is not possible and you have a technical support and maintenance contract then please submit a ticket to receive a patch.

Hanwha Techwin

[이슈 분석]

1. 현재 카메라 적용되어 있는 gSOAP 버전은 2.8.8 이며,
   gSOAP 2.8.24 버전까지 패치된 보안 이슈는 TLS 1.2 관련 이슈입니다.
   * TLS 1.1로 설정된 TLS 프로토콜을 TLS 1.2 까지 지원가능하도록 변경하였습니다.
   → 해당 내용은 Lighttp 웹서버에서 모두 처리되도록 하였기 때문에 해당 보안 이슈는 없습니다.

2. gSOAP 2.8.48 버전에 적용된 보안 이슈는 2GB 이상의 WSDL 데이터 전송 이슈입니다.
   → 해당 내용은 Lighttpd 웹서버에서 content length 가 검사되도록 해서 gSOAP서비스에 전달되도록 카메라에 적용되어 있기 때문에 해당 보안 이슈는 없습니다.

[결론]

gSOAP 관련 보안 이슈는 우리 카메라 제품에는 해당되지 않습니다.
그럼에도 불구하고, 현재 최신 버전이 적용 가능한지 개발팀에서 테스트 진행중에 있으며,
적용 가능함을 확인 후 향후 단계적으로 최신 버전 적용할 수 있도록 할 예정입니다.