Hanwha Techwin

July 25, 2017

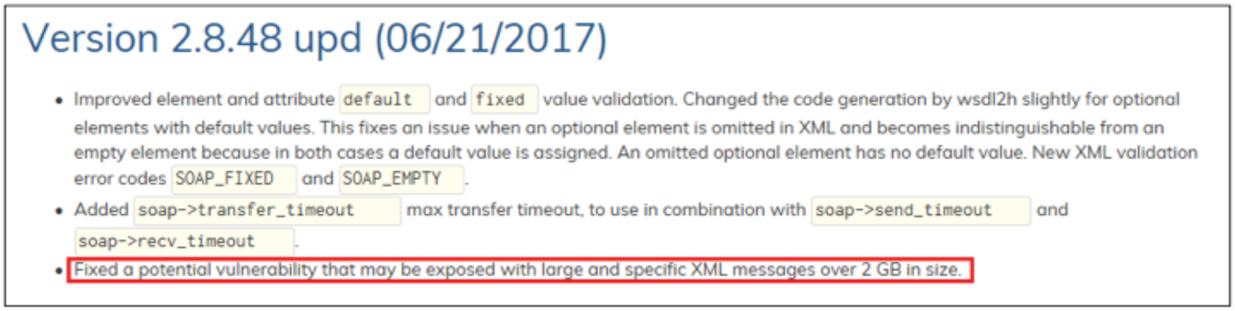
CVE-2017-9765

Vulnerability Report for gSOAP

[General Overview]

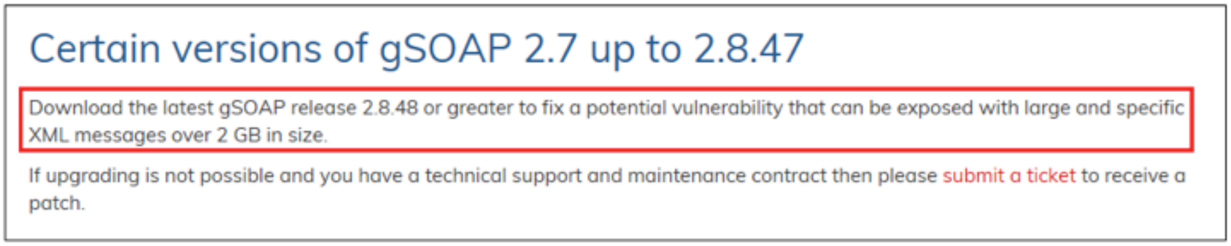
1. Hanwha Techwin was informed by the ONVIF technical committee that all ONVIF members who are using gSOAP versions lower than v2.8.48 should patch to the latest release to resolve a gSOAP vulnerability issue.
2. Hanwha Techwin devices are not impacted by the known vulnerability.
3. Genivia, licensor of gSOAP, released a patch to address this vulnerability at v2.8.48 on June 21, 2017.
   https://www.genivia.com/changelog.html
   https://www.genivia.com/advisory.html

[Vulnerability]
The vulnerability that was identified, may allow an attacker to crash the SOAP WebServices daemon (DOS-attack via specially constructed XML messages over 2GB). The flaw can also be exploited by a skilled and determined attacker to execute arbitrary code on the device.



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.



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.

[Risk Analysis]
Hanwha Techwin cameras and NVRs are not impacted by the recent, known gSOAP vulnerability as our devices filter the XML data prior to forwarding to gSOAP. All data communications pertaining to ONVIF web service that utilizes gSOAP library is run under our web server which prohibits direct client access to the gSOAP.

[Conclusion]
The known vulnerability mentioned in the advisory notice from Genivia does not affect Hanwha Techwin network devices and the advisory relating to the flaw of gSOAP is not relevant to our equipment. Therefore, no action is necessary for Hanwha Techwin users.

We will continue to monitor this situation, and any additional advisories from all parties, and continue to communicate all security updates to our customers.