Security Advisory: Polycom Web Configuration Utility Web Interface

Researched By: WootCloud IOT Threat Labs (WITL) **Date:** August 25th, 2018
(https://support.polycom.com/global/documents/support/user/products/voice/web_configuration_utility_ User_Guide.pdf)

Vulnerable Systems: PolyCom Web Configuration Utility
Issue 1: Authentication Credentials are Transmitted via Cookies in Encoded Format Details:

It has been observed that when session is initiated with the Polycom web configuration utility, it transmits the username and password in base64 encoded format. The credentials are then used with the "Authorization" header and are transmitted with every HTTP request. The security design flaw persists in the session cookies as these cookies use the stored encoded credentials as session tokens. The "Cookie Authorization" header carries the authentication credentials of the Polycom web configuration. Generally, storage of sensitive information in cookies is not considered as secure design. Even if the channel is encrypted, cookies can reveal information at several places. The design issue can be categorized into following CWE identifiers:

- CWE-522: Insufficiently Protected Credentials: https://cwe.mitre.org/data/definitions/522.html
- CWE-539: Information Exposure Through Persistent Cookies: https://cwe.mitre.org/data/definitions/539.html
- CWE-319: Cleartext Transmission of Sensitive Information: https://cwe.mitre.org/data/definitions/319.html
- CWE-312: Cleartext Storage of Sensitive Information: https://cwe.mitre.org/data/definitions/312.html

A POC is shown below:

```
GET /logConf.htm HTTP/1.1
Host   [IP Address]
User-Agent    Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101
Firefox/56.0
Accept */*
Accept-Language      en-US,en;q=0.5
Accept-Encoding      gzip, deflate
Authorization Basic UG9seWNvbTowd29vdGluZzA=
If-Modified-Since    [Truncated]11:12:46 GMT-0700 (Pacific Standard Time)
Referer      http://[IP Address]/index.htm
Cookie Authorization=Basic UG9seWNvbTowd29vdGluZzA=
Connection    keep-alive

HTTP/1.1 200 OK
Server Polycom SoundPoint IP Telephone HTTPd
Date   [Truncated]
Connection    keep-alive
Transfer-encoding    chunked
Content-type  text/html
```

Remediation

Sensitive information should not be allowed to be transmitted via cookies. Session tokens should not contain authentication credentials as part of cookie values.