**वीडियो कॉन्फ्रेंसिंग**

वीसी कैमरे, जो किसी भी पासवर्ड से सुरक्षित नहीं हैं या कमजोर पासवर्ड वाले हैं, का उपयोग चल रही वीडियो कॉन्फ्रेंसिंग में छिपने, कॉल की निगरानी करने, कॉल लॉग पढ़ने, वीसी के सीडीआर, चल रही कॉल में घुसपैठ करने/उसे बाधित करने आदि के लिए किया जा सकता है। इस भेद्यता का और अधिक उपयोग कैमरे को चालू करने और गतिविधियों पर नजर रखने के लिए रिमोट रखरखाव मॉड्यूल के माध्यम से किया जा सकता है। ऐसे हमलों को रोकने के लिए:

(i) वीसी कैमरे को प्रबंधित करने के लिए एक मजबूत पासवर्ड सेट करें।

(ii) रिमोट एक्सेस से एडमिनिष्ट्रेशन इंटरफेस को डिसेबल करें।

(iii) डिफॉल्ट खातों/पासवर्ड का उपयोग डिसेबल करें।

(iv) किसी भी गलत कॉन्फिगरेशन या गायब पैच का पता लगाने के लिए समय-समय पर जांच करें।

सरकारों और मूल भागीदार संगठनों के बीच विचार-विमार्श के लिए वाणिज्यिक वीसी समाधानों के सुरक्षित उपयोग के लिए:

(i) संगठन द्वारा एक अलग प्रणाली बनाई जा सकती है। ऐसी प्रणाली में कोई वर्गीकृत या संवेदनशील जानकारी संग्रहीत नहीं होनी चाहिए।

(ii) बैठक के लिए पृष्ठभूमि का चयन इस प्रकार किया जाना चाहिए (जैसे सादी दीवार, पर्दे या वीसी अनुप्रयोग का पृष्ठभूमि के विकल्प) वीसी के दौरान कोई संवेदनशील दस्तावेज/परिवेश दिखाई न दे।

(iii) जहां भी संभव हो, ऐसे वीसी के लिए एक अलग इंटरनेट कनेक्शन को प्राथमिकता दी जानी चाहिए। वीसी सिस्टम के लिए तार्किक अलगाव पर भी विचार किया जा सकता है ताकि अन्य आंतरिक सिस्टम वीसी नेटवर्क के संपर्क में न आएं।