Australian Government
Department of Defence
Intelligence and Security

CYBER SECURITY OPERATIONS CENTRE

PROTECT

NOVEMBER 2012

CONSUMER GUIDE: Emerson Network Power Avocent SC620, SC640, SC680, SC740, and SC780 Keyboard/Video/Mouse Switch

Product Description

1. The Emerson Network Power Avocent SwitchView SC620, SC640, SC680, SC740, and SC780 KVM products ('the products') provide the ability to use one console with up to eight different hosts. The SC640 is the direct replacement for the SC4UAD. These products provide separation between systems such that a single console can be used without the risk of data from one system transferring to another. The architecture of the switch isolates the data of each connected system at all times. The products implement dual-link DVI-I and USB connections. There are options for two, four, or eight port products with single or dual head video.

2. The Emerson Network Power Avocent SwitchView SC620, SC640, SC680, SC740, and SC780 KVM products may be used to share a console between systems of any classification.

Evaluation Scope and Summary

3. The scope of the evaluation included all functionality of the products.

4. The products have been awarded a High Assurance certification.

DSD Cryptographic Evaluation

5. There were no cryptographic components within the scope of the evaluation.

Conditions of Use

6. For Australian Government users, the following conditions must be adhered to for use between TOP SECRET or SECRET systems, and systems of a lower classification.

   a. The products may be used with analogue or digital video signals;

   b. The speaker functionality of the products may be used;

c. The microphone functionality must not be connected when spanning classifications, or where the accreditation of the facility housing the system exceeds that of any connected system. For example, if two SECRET systems housed in a TOP SECRET accredited facility are connected to the products, the microphone functionality must not be used;

d. Do not connect a KVM switch to another KVM switch; and,

e. The products must be housed in a facility accredited to process data to at least the level of the highest classified system connected to the products. For example, if a system accredited or classified as TOP SECRET is connected to the products, the surrounding facility must be accredited to process TOP SECRET data.

DSD's Recommendations

7. For Australian Government users, DSD makes the following recommendations:

a. users should select different passwords for each system connected to the products;

b. when switching between systems, the systems not being used should be locked;

c. where possible, label the system classifications on connected systems; and,

d. agencies should contact DSD before deploying the products overseas.

Contact Details

For further information regarding the certification of these products, or compliance with the ISM, please contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian Government Information Security Manual

The advice given in this document is in accordance with the *Australian Government Information Security Manual*, release date September 2012.

Date of this Consumer Guide

This Consumer Guide was issued by DSD on 1 November 2012.