Evaluation of Government Exposed Building Automation Systems

Brought to you by:

WhiteScope LLC and QED LLC

Concerns

- Exposure of devices to the Internet is the *number one risk* for building automation systems
  - Allows remote attacker to create cyber-physical effects
  - Provides potential access to corporate networks
  - Provides attack vectors to devices without detection
- Lack of capability to identify Internet facing devices
  - Multiple critical buildings exposed across myriad agencies
  - No insight into the magnitude of the risk or exposure

BASec: Government Facilities

- Over the past year
  - Scanned the Internet for building automation systems
  - Hundreds of exposed government facilities identified
  - Default configurations are the norm
  - Weak/default passwords and unpatched systems
  - Exposed devices extremely vulnerable to attack
- Reporting
  - List of exposed government facilities provided to DHS, GSA, GAO and DoD over the past year
  - Risk still exists
  - Who's role is it to accept responsibility

Top 10 – BAS Security Questions

- Are any our devices are facing the Internet? Have we confirmed?
- Are our devices patched with the latest version of vendor software?
- Do we know if any devices were recently replaced? If so, were they deployed matching our security policy?
- Are any of our old devices deployed to locations we longer manage?
- How do we audit our devices in a cost effective and repeatable way?

Top 10 – BAS Security Questions

- Are our devices configured securely, how can we verify?
- Do we have a security policy deployed to all of our devices?
- Are the log files being monitored for intrusion or malicious activity?
- How would we know if any of our devices have been compromised?
- How can we confirm the network segmentation or 'air gap' is secure?

Contact

http://smartbuildingsecurity.com

contact@whitescope.io

Questions?