CYBER SECURITY BULLETIN

USS-EDGE CYBER HARDENING

OVERVIEW

The FLIR USS Edge server is a compact appliance, equipped with 8 port built-in PoE switch, and is pre-loaded with Latitude VMS (Video Management System) installation files.

Cyber Security protection requires continuous adaptation to the ever-changing threats from cyber-attacks.

In order to increase the cyber hardening and in order to facilitate the out-of-the-box experience process, we have introduced several changes to the imaging process.

CYBER HARDENING DETAILS

FLIR USS-Edge machine is installed with Windows 10 Operating System (OS) and is being patched periodically with the latest OS updates. In addition, it is installed, configured and patched with the latest Latitude software updates.

The following steps have been added to the USS Edge staging process before shipping:

1. **Enable Windows Firewall** – Windows Firewall is now enabled and configured to allow proper functioning of Latitude VMS.
2. **Disable unused network protocols** such as Telnet, FTP and SSH.
3. **Disable SSL 3.0 & 2.0 & TLS 1.0** – these are deprecated protocols that may impose cyber security risks.
4. **Disable SMBv1** - SMBv1 is an old version of the Server Message Block (SMB) protocol that Windows uses for file sharing on a local network. Flaws in this protocol can be used to spread Malware and Ransomware, therefore it is important to disable this protocol. It's been replaced by SMBv2 protocol.
5. **Enable SMBv2** - SMB2 is a new version of the old Windows filesharing protocol SMB and is used for filesharing on modern and future Windows hosts.
6. **Set SMB Signing to be required** - SMB Signing is a feature through which communications, using SMB, can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity. This security mechanism in the SMB protocol helps avoid issues like tampering of packets and "man in the middle" attack.
7. **Run Windows Updates** – Windows OS was updated with the latest security updates available at the time of imaging.
8. **Include all cyber hardening steps introduced in previous bulletin** – see details at: https://www.flir.com/globalassets/security/cyber-security-bulletin---uss-and-meridian-hardening.pdf.

USE OF SQL SERVER 2017

As part of this update, we have changed the SQL Server version from SQL Server 2012 Express to SQL Server 2017 Express. Latitude VMS functionality was tested with this version and found to be working properly.

Cyber hardening Video Management Systems is necessary due to evolving cyber threats.

FLIR USS-Edge Appliance

19-1985-SEC-CyberBulletin_WebPosting 08/28/19