# FIVE STEPS TO MAKE A SECURE MEDICAL DEVICE

Mike Kijewski | mike@medcrypt.com | October 28, 2019

# 1. ACCEPT RESPONSIBILITY

MEDICAL DEVICE USERS ARE NOT SECURITY EXPERTS

RECALLS DISPROPORTIONATELY AFFECT MDMS

FDA NOW REQUIRES DEVICES TO BE SECURE BY DESIGN, BEFORE APPROVAL

# 2. THREAT MODEL

“WHY WOULD SOMEONE ATTACK THIS?” - NOT A RHETORICAL QUESTION

ASSESS PRIVACY, INTEGRITY AND CONFIDENTIALITY IN EQUAL PROPORTION

NEEDS TO HAPPEN DURING THE DESIGN OF THE DEVICE, NOT AFTER

# 3. SECURE BY DESIGN

NOW, BUYERS WANT SECURITY BUILT IN.

# 3. SECURE BY DESIGN

SECURE YOUR CONFIGURATION

ENCRYPT STUFF

SIGN STUFF

MONITOR BEHAVIOR IN THE FIELD

# 4. PATCH

## MEDCRYPT.COM/WHITEPAPERS

### THE MISSING LINK BETWEEN CYBERSECURITY VULNERABILITIES AND PATCHES

An analysis of ICS-CERT cybersecurity disclosures reveals **no correlation** between a vulnerability's CVSS score and the likelihood a patch will be made available by the manufacturer.





# THE MISSING LINK BETWEEN CYBERSECURITY VULNERABILITIES AND PATCHES

An analysis of ICS-CERT cybersecurity disclosures reveals **no correlation** between a vulnerability's CVSS score and the likelihood a patch will be made available by the manufacturer.

**Background:**

Throughout a software's lifetime, it will run into problems. A patch is the immediate fix to those problems.

In 2016, the FDA released the guidance document entitled Post-Market Management of Cybersecurity in Medical Devices, in which the FDA makes several recommendations to medical device vendors and healthcare delivery organizations on how to manage the cybersecurity risk that connected medical devices introduce. One of the recommendations is for device vendors to design devices to "anticipate software patches," in which the design of a device must consider the need for ongoing patching as well as a mechanism to rapidly deploy patches based on identified vulnerabilities.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has played a critical role in bringing visibility to emergent threats by building a repository for medical device manufacturers to communicate with customers. Assessing these alerts for patching attributes revealed a **50%** increase in frequency of patching vulnerabilities since the FDA has issued their guidance documen, but no correlation between CVSS scores and frequency of patching but **no correlation** between CVSS scores and frequency of patching.

## READERS WILL LEARN

| OBSERVATION | PREDICTIONS | FOR ADDITIONAL DETAIL |
|---|---|---|
| Regulatory Guidance Requires Patching Consideration in Device Architecting | Additional device vendors and vulnerability types will increase frequency of patching | Section I |
| Patching is Selectively Used as a Mitigation | Future disclosures across all device types will increase frequency of patching | Section II |
| Security Researchers Influence Patching | "Bar for patching" will lower, increasing volume of patching | Section III |
| Frequency of Patching has Increased, but Concentrated in Industry Leaders | Best patching practices will become required to compete in the marketplace | Section IV |

### A NOTE ON THE INCLUSION OF VENDOR NAMES:

It should be noted that the authors of this paper consider the inclusion of a specific medical device vendor's name in the list of companies below **to be a positive indicator** of their **active management** of cybersecurity risk. No piece of technology is completely devoid of cybersecurity risk, and so any manufacturer of a technology product should be expected to have to deal with managing cybersecurity vulnerabilities in their products from time to time. Medical device vendors who actively disclose and address cybersecurity vulnerabilities should not necessarily be seen as negligent for having a cybersecurity vulnerability, but rather should be applauded for addressing their vulnerabilities publicly.

**Patching medical devices informs system architecture designs, including connectivity, clinical and practitioner interaction. If you deal with a connected device, you will benefit from understanding the state of patching today.**

# 4. PATCH

- FDA EXPECTS PATCHING IN 60 DAYS
- PATCHES NEED TO BE AVAILABLE TO CUSTOMERS LONG AFTER “END OF SALE”
- NEED TO INCENT USERS TO APPLY PATCHES

# 5. DISCLOSE

ONLY 7 OF THE TOP 40 MDMS HAVE EVER RELEASED A DISCLOSURE

~40% OF DISCLOSURES ARE FROM PHILLIPS & BD

“WE MAY BE LOOKING TO REQUIRE COORDINATED VULNERABILITY DISCLOSURE THROUGH LEGISLATION IN ORDER TO LEVEL THE PLAYING FIELD.” - FDA

# FIVE ACTIONS YOU CAN TAKE

1. ACCEPT RESPONSIBILITY

2. THREAT MODEL

3. SECURE BY DESIGN

4. PATCH

5. DISCLOSE

# QUESTIONS?

mike@medcrypt.com | @mikekijewski

# WHY CAN'T EVERY MEDICAL DEVICE VENDOR IMPLEMENT PROACTIVE SECURITY TODAY?

Security features can be obsolete, before they even ship.

Security features compete for priority with clinical features.

Security is hard. Even CIA, Apple, and Google have made mistakes.

# AND, EXISTING TOOLS WEREN'T BUILT FOR THIS.

Monitoring tools for hospitals alert the hospital, not you, creating alarm fatigue.

Anti-virus software wasn't built with safeguards for keeping people alive.

Traditional IoT security software wasn't designed for clinical use.

# EASILY ADD PROACTIVE SECURITY TO ALL OF YOUR DEVICES— AND

BEST-PRACTICE SECURITY VIA MEDCRYPT IN AS FEW AS 9 LINES OF CODE

```
var data_for_webserver = “Hello”; //The data to be sent to “webserver”
var data_stiring;                 //The data after it is processed by the Guardian

data_string = guardian.dataFor(‘webserver’, data_for_webserver);
```

# THANK YOU

mike@medcrypt.com | @mikekijewski