Risks of Embedded Operating Systems on Medical Devices

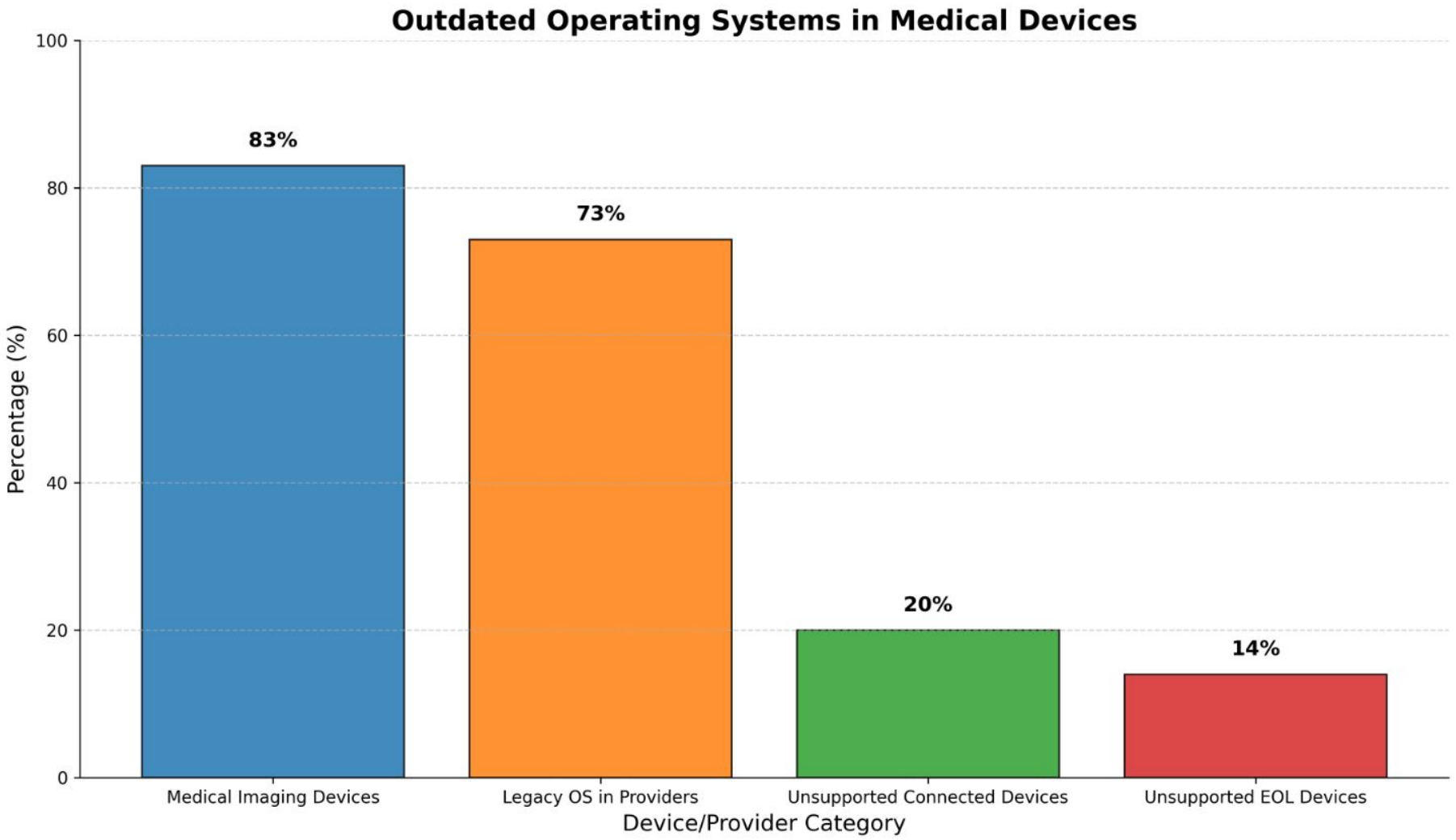
Samantha Paquette

What is an Embedded Operating System

- Specialized operating systems built into devices
- Designed for reliability, real-time performance
- Often invisible to users

- Examples:
  - Windows (XP, 7, 8, etc)
  - Linux
  - VxWorks
  - QNX

Outdated Operating Systems In Medical Devices



Real World Examples

Year	Event	OS / Device	Impact
2017	**WannaCry Ransomware**	Windows XP, other legacy OS	NHS hospitals disrupted; imaging & lab equipment frozen; delayed care
2015–2018	**MRI System Failures**	Windows XP Embedded	Machines froze mid-scan; delayed diagnostics
2018	**Lab Analyzer Vulnerabilities**	Windows 7 Embedded	Potential for tampered results or data theft
2016–2019	**Radiation Therapy Device Risks**	Unsupported Windows OS	Devices isolated from networks; reduced monitoring & efficiency
2017–2020	**Infusion Pump Cyber Flaws**	Windows XP Embedded	FDA recalls & security alerts; hospitals forced to mitigate

Why Medical Devices Run Older OS

- Long device lifecycles
- FDA/ Regulatory requirements
- Vendor-locked software and hardware
- Stability prioritized over changes

What “Outdated” Really Means

- End of vendor support
- No security patches
- Unsupported hardware drivers
- Unsupported OS = known, unpatched vulnerabilities

Cybersecurity Risks of Outdated Embedded OS

- Known exploits
- Malware and ransomware risk
- Often cannot run modern antivirus

Patient Safety and Clinical Impact

- Device crashes or freezes
- Delayed diagnostics or treatment
- Delayed repair
- Incorrect data display or loss
- Forced device downtime

Operational and Financial Impact

- Increased unplanned downtime
- Longer repair times
- Expensive repairs
- Emergency replacements

Regulatory and Compliance Concerns

- FDA cybersecurity guidance
- Joint Commission risk management
- CMS and data protection expectations
- Audit and documentation risks

Risk Mitigation Strategies

- Network segmentation
- Compensating security controls
- Vendor service contracts
- Lifecycle replacement planning

Role of HTM, IT, and Vendors

- HTM: asset tracking and lifecycle planning
- IT: network security and segmentation
- Vendors: OS support, patches, and upgrades

Signs a Medical Device May be Compromised

Unusual Behavior:
- Freezing, crashing, or unexpected restarts
- Slower performance than normal

Unexpected Network Activity:
- Communication with an unknown IP address
- Increased or unusual network traffic

Security Alerts or Log Changes:
- Antivirus or monitoring alerts
- Unrecognized login attempts or system log changes

Unauthorized Configuration Changes:
- Settings modified without approval
- Software or firmware changes not scheduled

Data or Output Irregularities:
- Incorrect readings or inconsistent results
- Missing or altered patient data

Immediate Response Steps

- Do not power off immediately (may destroy forensic evidence)
- Disconnect device from the network if it’s safe to do so
- Remove from clinical use to protect patient safety
- Notify IT Cybersecurity and HTM immediately
- Document the issue (time, symptoms, alerts, etc)

Investigation

- IT performs **network and malware analysis**
- Vendor may be required for **firmware or OS reimaging**
- Device may need **patching or security updates**
- Security team reviews **logs and potential data exposure**
- Lessons learned applied to **future device risk mitigation**

Recovery

- **System patching** – Apply security updates and patches to address vulnerabilities
- **Device restoration** – Return device to full operational functionality
- **Strengthen defenses** – Implement enhanced security controls to prevent recurrence
- **Documentation** – Record incident details, actions taken, and outcomes
- **Validation testing** – Verify device operates correctly and securely before clinical use
- **Return to service** – Safely reintroduce device to clinical environment with monitoring

Preventing Future Compromises

- Network segmentation for medical devices
- Regular vulnerability assessments
- Strong access control and authentication
- Continuous device monitoring
- Lifecycle replacement of unsupported systems

Medical Device Cyber Incident Response Flow

DETECT

- Unusual Device Behavior
- Security Alerts & Logs
- Suspicious Network Activity

Potential Compromise

CONTAIN

- Disconnect from Network
- Remove from Clinical Use
- Notify IT & HTM Teams

Immediate Actions

INVESTIGATE

- Forensic Analysis
- Firmware & OS Assessment
- Data Breach Evaluation

In-Depth Analysis

RECOVER

- System Patching
- Device Restoration
- Strengthen Defenses

LESSONS LEARNED

Improve Future Device Security

DOCUMENT INCIDENT → ANALYZE IMPACT → APPLY FIXES

Key Takeaways

- Embedded OS are critical but often invisible components of devices.
- Outdated OS increase risks to patient safety, cybersecurity, and operational efficiency.
- Upgrades are challenging, requiring coordination with vendors and IT.
- Mitigation strategies and proactive lifecycle planning are essential.
- HTM teams play a central role in ensuring devices remain safe, functional, and compliant.

Q&A / Discussion