OT Vulnerability Management

Identifying, prioritizing, and remediating vulnerabilities in industrial systems

OT Security Learning Series

Document 720 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 Vulnerability Management Lifecycle **3**

3 Vulnerability Identification **3**
3.1 Discovery Methods . . . 3
3.2 Vulnerability Sources . . . 4
3.3 Asset Correlation . . . 4

4 Risk-Based Prioritization **4**
4.1 OT-Specific Risk Factors . . . 4
4.2 Prioritization Matrix . . . 5
4.3 Priority Categories . . . 5

5 Remediation Strategies **5**
5.1 Remediation Options . . . 5
5.2 Patching Process . . . 6
5.3 Compensating Controls . . . 6

6 Managing Legacy Systems **6**
6.1 End-of-Life Challenges . . . 6
6.2 Legacy System Protection Layers . . . 7

7 Vulnerability Metrics and Reporting **7**
7.1 Key Metrics . . . 7
7.2 Reporting Cadence . . . 7

8 Program Implementation **7**
8.1 Success Factors . . . 8
8.2 Common Pitfalls . . . 8

9 Summary **8**

10 Further Reading **8**

1 Introduction

Information

Vulnerability management in OT environments requires balancing security with operational continuity. Unlike IT, where patches can often be applied quickly, OT systems may require extensive testing, vendor coordination, and scheduled downtime before vulnerabilities can be remediated.

OT vulnerability management challenges:

- **Availability priority:** Downtime for patching may not be acceptable
- **Legacy systems:** Many systems no longer receive security updates
- **Testing requirements:** Patches must be validated before deployment
- **Vendor dependencies:** May need vendor approval or assistance
- **Long lifecycles:** Systems operate for 15–30 years

2 Vulnerability Management Lifecycle

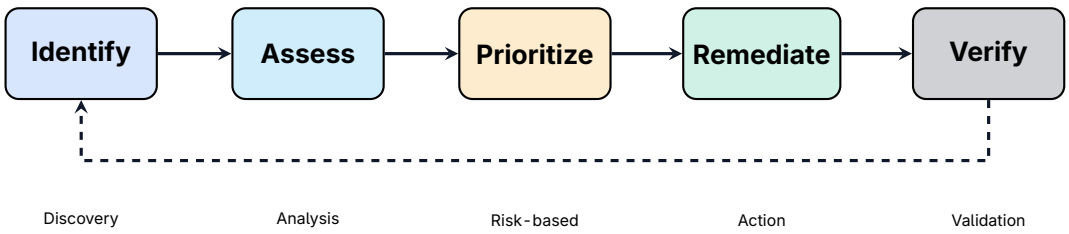

Figure 1: Vulnerability Management Lifecycle

3 Vulnerability Identification

3.1 Discovery Methods

Method	OT Suitability	Considerations
Passive scanning	Preferred	Network traffic analysis
Agent-based	Moderate	May impact performance
Active scanning	Use caution	Can crash legacy devices
Manual inventory	Safe	Labor-intensive
Vendor notifications	Recommended	Subscribe to advisories

Table 1: Vulnerability Discovery Methods for OT

Warning

Active Scanning Risks:

- Legacy PLCs may crash when scanned
- Network scanning can disrupt real-time communications
- Some devices reboot when receiving unexpected packets
- Always test scanning tools in lab environment first

3.2 Vulnerability Sources

- **ICS-CERT/CISA advisories:** US government OT vulnerability alerts
- **Vendor security bulletins:** Direct from equipment manufacturers
- **CVE databases:** National Vulnerability Database (NVD)
- **Security researchers:** Published vulnerability disclosures
- **Internal assessments:** Penetration tests, security audits

3.3 Asset Correlation

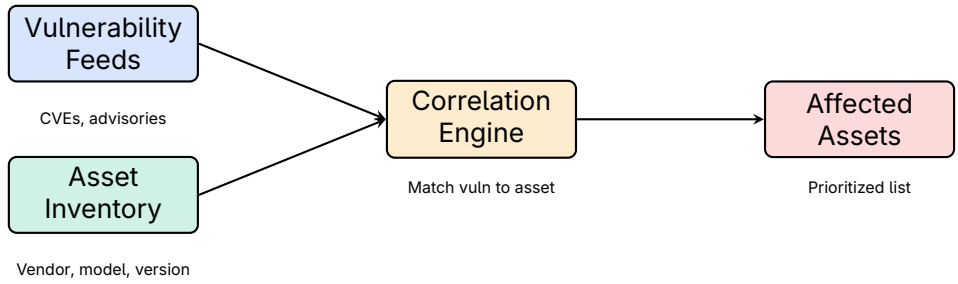

Figure 2: Vulnerability-to-Asset Correlation Process

Key Point

Accurate asset inventory is essential: You cannot determine which vulnerabilities affect your environment without knowing exactly what hardware, software, and firmware versions are deployed.

4 Risk-Based Prioritization

4.1 OT-Specific Risk Factors

Standard CVSS scores may not reflect true OT risk. Consider additional factors:

Factor	OT Consideration
Safety impact	Could exploitation cause physical harm?
Production impact	What is the cost of downtime or damage?
Asset criticality	Is this a safety system, core process, or support?
Exposure	Is the vulnerable system internet-accessible?
Exploitability	Is there a public exploit? Active exploitation?
Compensating controls	Is the system isolated, monitored, protected?

Table 2: OT-Specific Risk Prioritization Factors

4.2 Prioritization Matrix

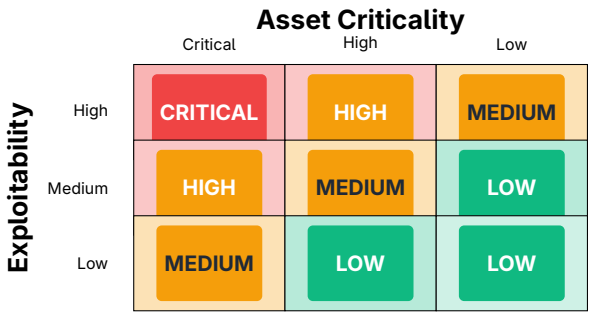

Figure 3: Risk Prioritization Matrix

4.3 Priority Categories

- CRITICAL **Immediate action:** Safety systems, actively exploited, internet-exposed
- HIGH **Urgent (days):** Core process control, public exploit available
- MEDIUM **Planned (weeks):** Important systems, no active exploitation
- LOW **Scheduled (months):** Low-impact systems, difficult to exploit

5 Remediation Strategies

5.1 Remediation Options

Option	When to Use	OT Consideration
Patch/Update	Vendor provides fix	Requires testing, downtime
Compensating control	Patch unavailable/risky	May not fully address risk
Network isolation	Cannot patch	Limits connectivity
System replacement	End-of-life, critical vuln	Expensive, time-consuming
Risk acceptance	Low risk, high cost	Document decision

Table 3: Remediation Options for OT Vulnerabilities

5.2 Patching Process

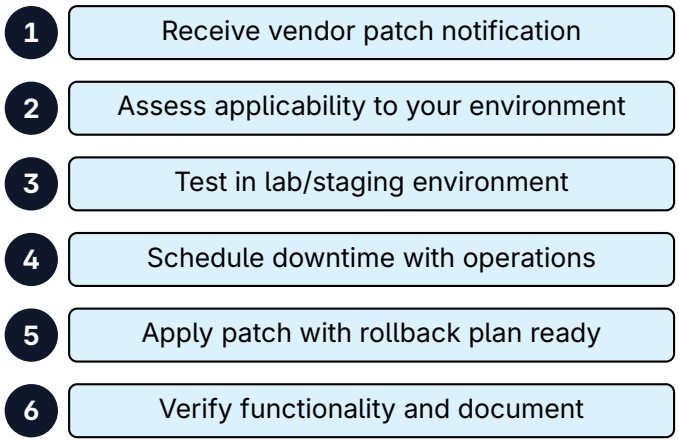

Figure 4: OT Patching Process

5.3 Compensating Controls

When patching is not possible:

Warning

Compensating Controls for Unpatchable Systems:

- Network segmentation (firewall, VLAN isolation)
- Data diodes for one-way communication
- Application whitelisting on connected systems
- Enhanced monitoring and alerting
- Physical access restrictions
- Disable unnecessary services and protocols

6 Managing Legacy Systems

6.1 End-of-Life Challenges

Critical

Many OT systems operate beyond vendor support. When patches are no longer available:

- Document the risk formally
- Implement maximum compensating controls
- Plan for eventual replacement
- Monitor for exploitation attempts
- Consider third-party security support

6.2 Legacy System Protection Layers

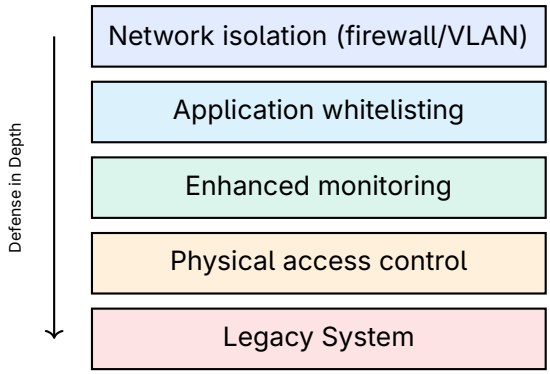

Figure 5: Protection Layers for Legacy OT Systems

7 Vulnerability Metrics and Reporting

7.1 Key Metrics

Metric	Description
Open vulnerabilities by severity	Count of unresolved vulns by priority
Mean time to remediate (MTTR)	Average time from discovery to fix
Patch coverage	Percentage of systems at current patch level
Compensating control coverage	Systems protected when patching impossible
Overdue vulnerabilities	Vulns past SLA for remediation
Risk reduction trend	Change in overall risk exposure over time

Table 4: Vulnerability Management Metrics

7.2 Reporting Cadence

- **Daily:** New critical vulnerabilities, active exploitation alerts
- **Weekly:** Vulnerability status, upcoming patch activities
- **Monthly:** Trends, metrics, risk posture summary
- **Quarterly:** Executive summary, program effectiveness

8 Program Implementation

8.1 Success Factors

Key Point

Building an Effective OT Vulnerability Program:

1. **Executive support:** Security competes with production priorities
2. **OT/IT collaboration:** Combined expertise required
3. **Accurate asset inventory:** Foundation for everything
4. **Realistic SLAs:** Account for OT patching constraints
5. **Testing capability:** Lab environment for patch validation
6. **Clear escalation:** Process for unacceptable risk decisions

8.2 Common Pitfalls

- Applying IT patching timelines to OT (unrealistic)
- Active scanning without understanding OT impact
- Ignoring compensating controls as valid remediation
- Lack of vendor coordination
- No lab environment for testing

9 Summary

Key Takeaways

- **OT patching is different:** Requires testing, coordination, downtime
- **Asset inventory essential:** Cannot match vulns without it
- **Risk-based prioritization:** CVSS alone insufficient for OT
- **Multiple remediation options:** Patching, compensating controls, isolation
- **Legacy systems:** Protect with defense-in-depth when patches unavailable
- **Metrics matter:** Track progress and demonstrate risk reduction

10 Further Reading

Standards

- **IEC 62443-2-3** – Patch management in the IACS environment
  https://webstore.iec.ch/publication/7032
- **NIST SP 800-82 Rev. 3** – Guide to OT Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA ICS Advisories**
  https://www.cisa.gov/news-events/ics-advisories
- **National Vulnerability Database**
  https://nvd.nist.gov/

Part of the OT Security Learning Series