ICS-Patch

What To Patch When In ICS?

A Decision Tree Approach

Version 0.5 – 13 Sept 2020

Introduction

Applying security patches is part of a cybersecurity program, which is an element of a risk management program. The goal of an organization is not to have fully patched cyber assets. It is to manage risk to an acceptable level. Security patches should be applied when they are the most efficient and effective way to reduce risk to an acceptable level.

The ICS-Patch project was created to assist ICS asset owners with the decision of what to patch when. The project had two main goals:

1. To make the decision on what to patch when in an asset owner's ICS based on each security patches contribution to risk reduction.
2. To automate the decision process of what to patch when so that no human interaction is required after setup for the ICS-Patch process to provide the recommended patching decision for each available security patch.

The automation does not mean that security patches are automatically applied, and the ICS asset owner may choose to perform further analysis on selected security patches. The ICS asset owners change control processes should drive the application of security patches.

There are key differences between a typical ICS cyber asset and an enterprise cyber asset that make the decision of what to patch when in ICS different than in the enterprise.

- Many of the ICS cyber assets are insecure by design. Documented features and functions provide an attacker with all the capabilities they would want on the cyber asset. Vulnerabilities are not required to cause the consequence, and therefore applying security patches typically results in minimal risk reduction. This is recognized in the Security Posture Change decision point.
- An ICS is a special purpose application to monitor and control a physical process. It is not used, or allowed to, receive email, browse web sites, or use a wide variety of applications. An ICS cyber asset is typically more difficult for an attacker to access than a cyber asset on the Enterprise. This is recognized in the Exposure decision point.
- The physical processes controlled by many ICS have the potential to cause harm to or the loss of human life. Safety controls are in place to reduce the risk to human safety to an acceptable level. A cyber attack on the ICS could potentially compromise the safety controls so they will not perform properly. This is recognized in the Safety decision point.
- Most ICS cyber assets and the ICS itself are static, rarely changing as compared to the typical enterprise cyber asset and enterprise network. This allows most of the decision points to be static and pulled from the asset inventory.

ICS-Patch Approach

ICS-Patch uses a decision tree to determine whether applying a security patch on an ICS cyber asset should be deferred, scheduled or applied as soon as possible (asap). Each node / decision point in the decision tree moves the ICS-patch process closer to the patch application decision.

All but one of the decision point values for an ICS cyber asset are expected to be static, entered when the cyber asset is placed into the asset inventory and rarely, if ever, changed. The Technical Impact decision point is related to the vulnerability being patched, and the CVSS score for the CVE is used to set this at a High, Medium or Low value. This makes the automation of the what to patch when question simple.

- The US National Vulnerability Database (NVD), or a similar feed, would be used along with an ICS asset inventory to identify if a patch applies to a cyber asset and to identify the Technical Impact decision point for the security patch.
- The remaining decision point values would be extracted from the ICS asset inventory for the cyber asset who the security patch applies to.
- The decision point values are input to the decision tree, and the recommended security patch action (defer, schedule or asap) is output.

This ICS-Patch decision tree could be run in the asset inventory / asset management product, in a vulnerability management application, or in a separate application.

Decision Tree Results

The ICS-Patch decision tree will lead to one of three results for each cyber asset / security patch pair.

Defer
Do not apply or schedule to apply the security patch on the cyber asset for risk reduction. (The asset owner may choose to apply the security patch as part of cyber maintenance to keep the system under support.)

Scheduled
The security patch should be applied on the cyber asset during the next scheduled patch window. For some ICS, this may be a scheduled outage that occurs annually or semi-annually. For others they may choose a quarterly or monthly patching interval.

ASAP
Apply the security patch on the cyber asset as soon as possible in a safe manner.

Decision Points

The nodes in the decision tree are decision points that will determine what branch the security patching decision will flow down. Each decision point represents a factor that will affect the "what to patch when" risk-based decision, and there are three possible values for each decision point. Restricting each decision point to just three values recognizes the limited precision available in determining the values of the decision points, as well as the limited value to the risk-based decision process in additional precision.

The decision points and values are defined below.

Exposure

The Exposure of the ICS cyber asset to attacks is first decision point in the decision tree. If it is very difficult for an attacker to gain access to the cyber asset, then applying the security patch results in less reduction. In addition, if the attacker is able to gain access to a highly trusted zone, such as Level 2 or 1 in the Purdue Model, then the insecure by design nature of the protocols and Level 1 devices would render the value of an exploit for an unpatched vulnerability much lower.

Small:
The cyber asset is in a highly isolated and controlled zone. There are no connections from this cyber asset's zone to or from a zone with lower trust.

Indirect:
The cyber asset has no direct access to a zone with lower trust, but other cyber assets in this cyber asset's zone are accessible to or from a zone with lower trust.

Direct:
The cyber asset is directly accessible to or from a zone with lower trust.

Source: The Exposure will be based on the cyber asset and should be a field in the Asset Inventory. Exposure is expected to rarely change.

Architecture Notes: The architecture should not allow any Exposure:Direct to a cyber asset that is Safety Impact:Direct.

The architecture should not allow any Exposure:Direct to a cyber asset that is Process Impact:Essential Failure.

The architecture should minimize the number of assets in the Exposure:Direct.

The architecture should not allow any Exposure:Direct to Security Posture:Trivial

Additional Consideration: A cyber asset with Exposure:Direct may consider whether the security patch under evaluation would prevent a vulnerability from being exploited from the less trusted zone. In other words, Exposure:Direct could be based on the cyber asset attack service accessible from the less trusted zone rather than simply classifying any access from a less trusted zone as placing the cyber asset in Exposure:Direct for all security patch evaluation. The downside of this approach is it is difficult to automate.

Safety Impact

Many processes being controlled and monitored by an ICS also have some cyber safety components that prevent the harm or loss of human life. This decision point is based on the connectivity or access of the cyber asset in the ICS and safety related cyber assets.

None: The vulnerability, if exploited, will not impact the safety of the process being monitored and controlled.

Indirect: The vulnerability, if exploited, will not directly impact the safety of the process being monitored and controlled. The attack would be required to compromise additional systems to have an impact on process safety.

Direct: The vulnerability, if exploited, would allow an attacker to modify or disable safety controls so they could no longer perform their function.

Source: The Safety Impact will be based on the cyber asset and should be a field in the Asset Inventory. Safety Impact is expected to rarely change.

Security Posture Change

Many, if not most, ICS cyber assets are in a highly insecure state prior to a security patch being evaluated. This could be due to the insecure by design nature of the cyber asset or the ICS protocols in use. It also could be due to a large amount of missing security patches in the operating system, application, libraries, protocol stacks, and other third party software, due to lack of vendor approval for applying security patches. If applying the security patch being evaluated will not make it more difficult for an attacker to achieve their goal, then the risk reduction value of applying the security patch is minimal. This consideration is addressed in the Security Posture Change decision point.

Trivial: The cyber asset is in a highly insecure state and additional vulnerabilities do not affect the ease of exploit or post exploit actions. (example: insecure by design PLC or a large number of missing security patches)

Minor: The cyber asset's maintenance schedule and typical security posture has it in a state that would be exploitable by a moderately skilled attacker with unfettered network access.

Major: The cyber asset is maintained in a secure posture with good security practices. The missing security patch is the best, and possibly only, method to compromise the cyber asset.

Source: The Security Posture Change will be based on the cyber asset and should be a field in the Asset Inventory. The Security Posture Change level for a cyber asset should remain static unless there is a change in the ICS security patching program.

Process Impact

The Process Impact decision point is related to the cyber asset's role in the process. The decision point is based on the impact to the process if the cyber asset is not available or lacks integrity.

Non-Essential Degraded: Little to no impact. Degradation of non-essential functions; chronic degradation could eventually harm essential functions.

Essential Degraded: Activities that directly support essential functions are degraded or crippled, but the process can continue to operate for some time.

Essential Failure: Activities that directly support essential functions are unavailable, and this leads to the process no longer operating properly.

Source: The Process Impact will be based on the cyber asset and should be a field in the Asset Inventory. Process Impact is expected to rarely change.

Technical Impact

The Technical Impact decision point is the only decision point that requires an external source, not the asset inventory, for the data. The CVSS score was selected as this is a widely available value and is integrated into many asset management / vulnerability management solutions.

Low: CVSS score between 0 – 3.9

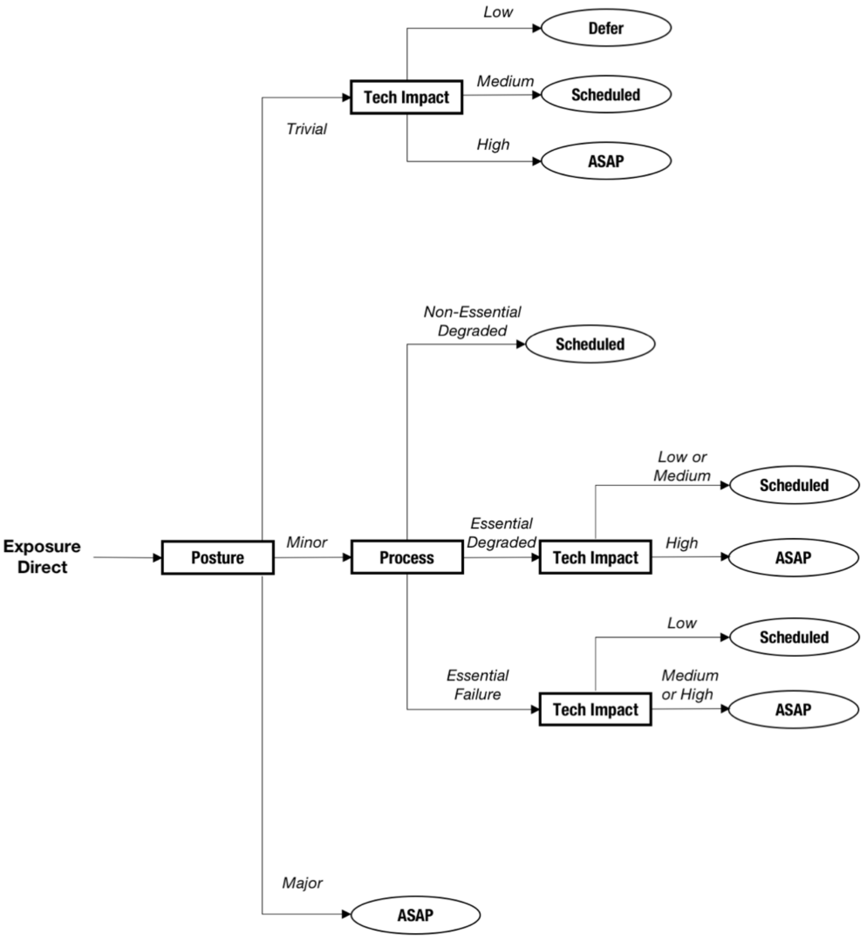
Medium: CVSS score between 4.0 – 6.9

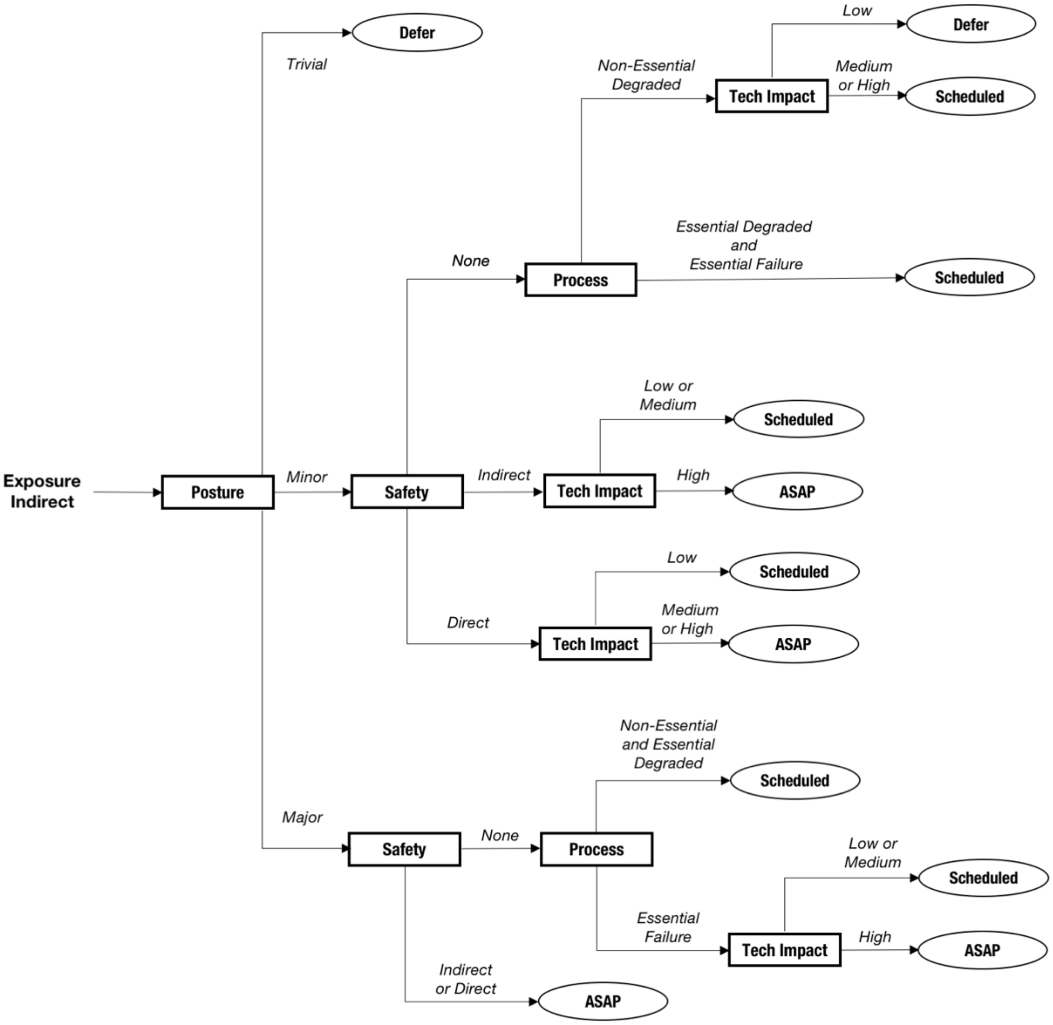
High: CVSS score between 7.0 – 10.0

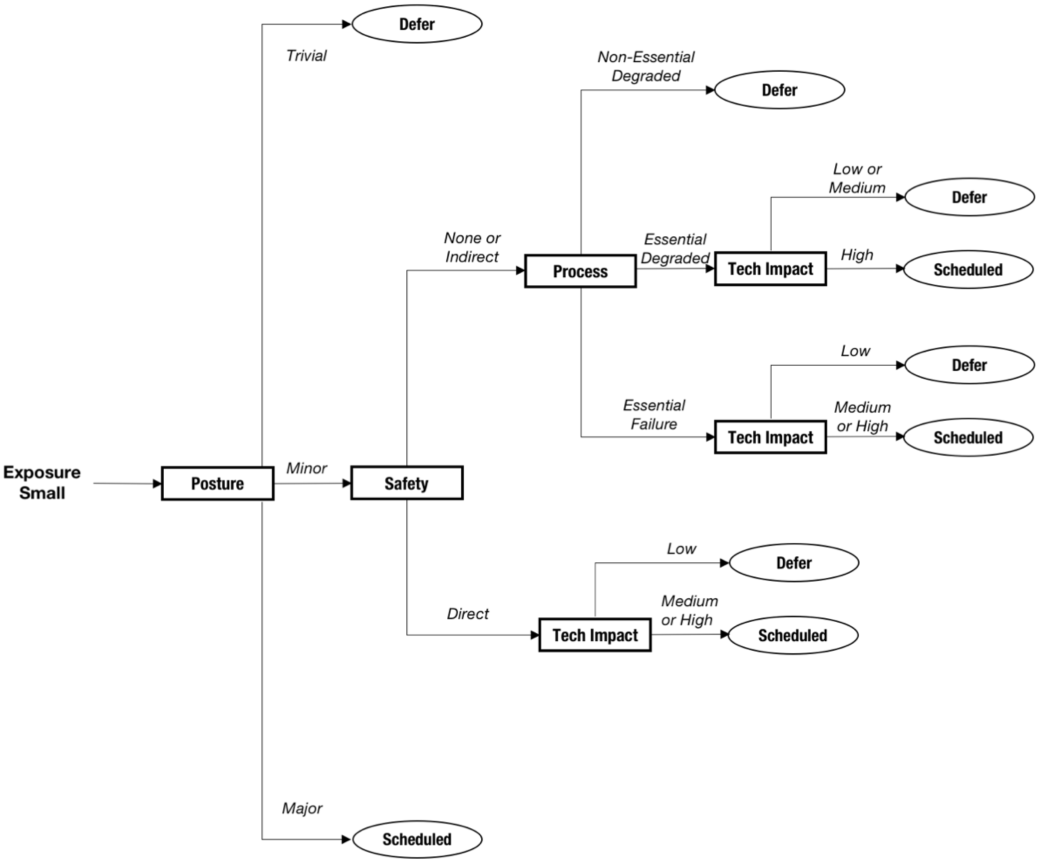
Source: The CVSS score can be pulled from a number of feeds, for example the NVD.

Decision Trees

The decision tree is shown in the three figures below. Each figure represents one of the Exposure decision point values. This was done to make the decision tree more readable. The entire decision tree could be viewed by placing the three figures in a vertical column and have an Exposure decision point to the left of these three pages.




Exposure Indirect
Posture
Trivial
Defer
Minor
Safety
None
Process
Non-Essential Degraded
Tech Impact
Low
Defer
Medium or High
Scheduled
Essential Degraded and Essential Failure
Scheduled
Indirect
Tech Impact
Low or Medium
Scheduled
High
ASAP
Direct
Tech Impact
Low
Scheduled
Medium or High
ASAP
Major
Safety
None
Process
Non-Essential and Essential Degraded
Scheduled
Essential Failure
Tech Impact
Low or Medium
Scheduled
High
ASAP
Indirect or Direct
ASAP



Relation to SEI's SSVC

Variations from the SEI/CERT SSVC.

Decision Tree Results

ICS-Patch has three categories as compared to the SSVC four categories. The SSVC categories of Out-of-Band and Immediate have been combined to ASAP.

Exploitation

There is no reliable and easily available source of information on whether an ICS security vulnerability is being exploited. Therefore, Exploitation is removed from the decision tree.

Exposure

The SSVC levels of Controlled and Unavoidable have been changed to Indirect and Direct in ICS-Patch.

Mission Impact

The SSVC four levels have been reduced to three, and the names and definitions of the two higher levels have been changed. The decision point Mission Impact has been changed to Process Impact as this is what is under consideration in ICS-Patch.

Utility

Similar to Exploitation, there is no source for this criterion. It is not included in the ICS-Patch decision tree.

Safety Impact

The SSVC has four levels of Safety Impact and the ICS-Patch has three. The SSVC level of Hazardous has been removed. Major would encompass what SSVC called Major and Hazardous.

Security Posture Change

This criterion was not included in the SSVC. It is more important in ICS given that many of the cyber assets are insecure by design and a vulnerability, whether patched or unpatched, would not appreciably affect risk.

References

We will add the references to the SEI document and S4 videos.