`

COST: **$**$$$ IMPACT: **HIGH** COMPLEXITY: **MEDIUM**

1.E: Does the WWS patch or otherwise mitigate known vulnerabilities within the recommended timeframe?

Recommendation: Identify and patch vulnerabilities in a risk-informed manner (e.g., critical assets first) as quickly as possible.

Why is this control important?

This control is important because it reduces the chances of attackers taking advantage of published vulnerabilities to breach your computer systems.

A vulnerability is a weakness in a piece of software or firmware running on a hardware asset. Vulnerabilities can come from mistakes in code or oversights in the software design process, or attackers may intentionally place vulnerabilities in software as a vendor writes the code (i.e., a supply chain attack). An exploit is either a set of actions or a piece of malicious code that attackers use against the vulnerability, helping them breach a computer system or damage an asset.

The original creator of software will provide a new version that does not contain the same weakness. Installing this software update is known as “patching” a system and upgrading to the new version prevents an attack from “exploiting” the known vulnerability.

Implementation Tips

You can use your Asset Inventory (see Factsheet 1.A), Configuration Documentation (see Factsheet 2.O), and the resources below to identify vulnerabilities that exist in your system. For IT assets, automated updates and patches are often already enabled (e.g., Windows updates). But for OT assets, the WWS often disables automated updates and patches. Therefore, a WWS may need to manually apply updates and patches for OT assets based on availability and operational feasibility. If a patch is not available or would unacceptably disrupt your WWS operations, you can use mitigating controls such as Network Segmentation (see Factsheet 2.F).

Additional Guidance

- ✓ For assets where patching is not feasible, apply compensating controls like segmentation (i.e., digitally separating the network into smaller pieces, each protected from the other) and enhanced monitoring (e.g., installation of network traffic monitoring tools).
- ✓ Acceptable measures either make the asset unreachable from the public Internet or reduce the ability of attackers to use the vulnerability in a cyberattack.

The U.S. federal government maintains several software vulnerability data resources and can send alerts about new entries to these databases. The most important is the Known-Exploited Vulnerability (KEV) database published by DHS CISA, containing information about vulnerabilities that attackers are already using. Any vulnerabilities on the KEV should receive the highest degree of prioritization. The National Vulnerability Database (NVD) published by NIST contains information about all publicly known vulnerabilities. Your utility should also register to receive alerts and advisories from DHS on new vulnerabilities. WaterISAC members also receive cybersecurity threat notifications, including critical vulnerabilities.

To automate the process of identifying vulnerabilities, DHS CISA offers free services for Internet-facing systems (see Factsheet 2.W) and many vendors offer paid vulnerability scanning tools and services for internal computer systems. To aid in vulnerability identification, your WWS can use a vulnerability scanner in the IT network and a passive monitoring tool in your WWS OT network.

WWS IT Systems

For the front-side business network, vulnerability and patch management can generally align with standard IT network practices, with only limited exceptions. This approach allows for the more frequent and routine application of updates and patches, typical of IT environments, leveraging automated systems and rapid deployment capabilities. It is important, however, to recognize and plan for any exceptions specific to the business network that might require deviations from these standard procedures. Tailoring patch management to accommodate these exceptions ensures that security and operational efficiency are maintained without compromising the unique needs of the business network. This strategic alignment should be explicitly documented in organizational cybersecurity policies to provide clear guidance on handling exceptions while adhering to best practices in IT security management.

WWWS OT Systems

Unlike IT systems, OT systems require tailored approaches due to dependencies on third-party vendors and the potential operational disruptions from frequent updates. Therefore, it is recommended to establish regularly scheduled maintenance windows coordinated with third-party vendors, utilizing planned disruptions to implement and test patches. Additionally, it is crucial to have support agreements in place that cover both scheduled and emergency interventions, and to deploy compensatory controls to mitigate risks until such updates can be safely applied. These practices should be linked to broader strategic cybersecurity goals to ensure a comprehensive approach to maintaining operational integrity while managing security risks.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SI-2 (page 333) and RA-5 (page 242) for more information on “Flaw Remediation” and “Vulnerability Monitoring and Scanning”. *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

`

NIST Policy Management Template Guide: See Patch Management (4.0 Information statement). A template that utilities can use to build a patch management strategy. *https://www.cisecurity.org/wp-content/uploads/2020/06/Patch-Management-Standard.docx*

DHS CISA Known-Exploited Vulnerabilities (KEV): See this resource for vulnerabilities that attackers have already exploited. *https://www.cisa.gov/known-exploited-vulnerabilities-catalog*

NIST National Vulnerability Database (NVD): See this resource for a list of publicly known vulnerabilities*.* *https://nvd.nist.gov/vuln/search*

DHS CISA Alerts: See this resource to sign up for email alerts from DHS CISA's National Cyber Awareness System regarding new vulnerabilities. *https://www.cisa.gov/uscert/ncas/alerts*

WaterISAC: See this resource for more information about the Water Information Sharing & Analysis Center (ISAC*).* *https://www.waterisac.org/*

CISA's Top Cyber Actions for Securing Water Systems: See item 7 on page 2 of this resource for additional information. *https://www.cisa.gov/resources-tools/resources/top-cyber-actions-securing-water-systems*