CISA INSIGHTS CYBER

Remediate Vulnerabilities for Internet-Accessible Systems

AT-A-GLANCE RECOMMENDATIONS

- Ensure Your Vulnerability Scanning Service is Scanning All Internet-Accessible IP Addresses
- Notify the Scanning Service of Any Modifications to Your Organization’s Internet-Accessible IPs
- Ensure the Scanning Service Provides At Least Weekly Scanning Results
- Coordinate with System Owners to Remediate Vulnerabilities

CYBERSECURITY THREAT

Adversaries operating in cyberspace can make quick work of unpatched Internet-accessible systems. Moreover, the time between an adversary’s discovery of a vulnerability and their exploitation of it (i.e., the ‘time to exploit’) is rapidly decreasing. Industry reports estimate that adversaries are now able to exploit a vulnerability within 15 days (on average) of discovery. After gaining entry into information systems and networks, these adversaries can cause significant harm.

Internet-accessible information systems include any system that is globally accessible over the public internet (i.e., has a publicly routed internet protocol (IP) address or a hostname that resolves publicly in DNS to such an address) and encompass those systems directly managed by an organization, as well as those operated by a third-party on an organization’s behalf. As organizations continue to expand their Internet presence through increased use and operation of interconnected and complex Internet accessible systems, it is more critical than ever to rapidly remediate vulnerabilities inherent to these systems. Failure to do so could allow malicious actors to compromise networks through exploitable, externally-facing systems.

The Cybersecurity and Infrastructure Security Agency (CISA) encourages its State, Local, Tribal and Territorial (SLTT) government partners, as well as private sector owners of critical infrastructure, to use this guide to learn more about this threat and associated mitigation

activities. This guidance is derived from Binding Operational Directive 19-02 – Vulnerability Remediation Requirements for Internet-Accessible Systems and includes lessons learned and additional considerations for non-federal entities seeking to implement actions in line with federal civilian departments and agencies, as directed by CISA.

RECOMMENDED ACTIONS

To ensure effective and timely remediation of vulnerabilities identified through vulnerability scanning, organizations should undertake the following actions:

Action 1: Ensure Your Vulnerability Scanning Service is Scanning All Internet-Accessible IP Addresses

- Create and maintain an asset inventory of all such IPs belonging to your organization.

Action 2: Notify the Scanning Service of Any Modifications to Your Organization's Internet-Accessible IPs.

- This includes newly acquired IPs or re-assigned IPs that are no longer part of your organization's asset inventory.

Action 3: Ensure the Scanning Service Provides At Least Weekly Scanning Results

Action 4: Coordinate with System Owners to Remediate Vulnerabilities

- CISA recommends the following remediation timelines:
  - Critical vulnerabilities should be remediated within 15 calendar days of initial detection.
  - High vulnerabilities should be remediated within 30 calendar days of initial detection.
- If vulnerabilities cannot be remediated within the recommended timeframes, develop a remediation plan for action and coordination across the organization. The remediation plan should include:
  - Vulnerability remediation constraints
  - Interim mitigation actions to overcome constraints
  - Final actions required to remediate vulnerability

LESSONS LEARNED AND ADDITIONAL CONSIDERATIONS

Lessons Learned

- The decentralization of organizations and their governance processes makes it difficult to coordinate the remediation of vulnerabilities. Network owners should be aware of who is operating their respective networks, if not done in-house.
- Without a clear understanding of an organization's internet-accessible footprint, it is not only difficult to identify anomalies, risks, and misconfigurations but also it is impossible to defend against what one does not know.
- Many organizations lack robust patch and configuration management policies and procedures to guide the coordination of vulnerability management-related activities at an operational level.
- Historically, most vulnerabilities identified by CISA are related to unsupported operating systems that cannot receive patched or upgraded (secure) software. This is largely due to the prevalence of legacy systems across all industries and sectors, some of which perform mission critical functions. The continued presence of end-of-life (EOL) systems is mostly due to the budgetary constraints inherent in replacing large amounts of EOL systems, often at the reduced funding levels of sub-organizations.

Implementation Considerations

- Establishing a coordination POC can help ensure the streamlined dissemination of vulnerability information to all sub-organizations. A coordination POC can also help resolve false positive claims and unnecessary remediation actions.
    - CISA's process for resolving false positives includes:
        1. Submit an email to your organization's coordination POC with analysis and supporting evidence for determination (for example, a screenshot of the IP address and operating system). CISA also utilizes a False Positive Assertion form for system owners to fill-out and submit to the coordination POC.
        2. The coordination POC facilitates review of the evidence and analysis to validate the assertion. This does not include exploiting a vulnerability, but may include actively sending packets to the host in question. If the analysis confirms the assertion, the vulnerability is marked as a false positive.
        3. False positive status expires 365 days after designation and personnel are required to re-submit evidence on an annual basis to confirm the vulnerability remains a false positive.
- Manage and prioritize cybersecurity risk appropriately within your environment. The nuances of each organization's environmental risk factors and mitigating controls is different. Prioritize certain vulnerabilities and devices over others in line with your organization's existing security baselines.
- Apply additional parameters, rules, and internal policy decision points as necessary, which may affect the acceptable timeframes to remediate specific types of vulnerabilities or vulnerabilities affecting certain types of devices. For example, organizations should consider the impact the exploitation of a vulnerability may have if an Internet-accessible IP is associated with a High Value Asset (HVA) or Mission Essential System (MES). Likewise, organizations should consider how many assets are affected by a specific vulnerability type and how long vulnerabilities have existed.
- Continuously analyze threat information, vulnerability information, and engage sub-organizations to further prioritize actions which may go beyond the defined scores to indicate 'critical of critical' vulnerabilities. In these instances, provide alerts to sub-organizations to ensure adequate steps are being taken across the organization.
- Not every vulnerability will require immediate action, nor is it prudent to apply patches without first analyzing and testing to minimize disruption to network operations. In these cases, organizations should clearly articulate the rationale for not remediating the vulnerability to the group coordinating organization-wide vulnerability management.
- Where patching is not possible due to certain limitations, network segregation is highly recommended to limit exposure of the vulnerable system or host.

Vulnerability Scanning Considerations

- Ensure a service agreement is established and signed between your organization and the scanning service provider to outline the scope and parameters of scanning.
- Include all in-scope IPs from all aspects of the organization (i.e., sub-organizations) in the IP asset inventory to ensure scanning and vulnerability identification across the organization. If ports aren't normally open to the general public (e.g. only certain whitelisted IPs can connect), you should still ensure the IP is included in the scanning scope so the scanning service can act as a double-check on that rule for you.
- Ensure scanning access by removing the service's source IP addresses from block lists. This allows your organization to properly triage and respond to alerts generated by your Security Information and Event Management (SIEM). These addresses may change without prior notice, so CISA recommends regular monitoring of any provided source IP list.
- Ensure Internet Service Providers (ISPs), Cloud Service Providers (CSPs), and other shared service providers are aware of your organization's requirements for remediating internet-accessible vulnerabilities. Ensure service providers are meeting or exceeding remediation requirements.

- Do not grant preferential treatment (e.g. explicitly whitelisting or opening any ports/services other than what is normally available for your systems) for the scanning. This allows the scanning service to find and report on vulnerabilities from a perspective similar to that of an attacker. However, scanning services are focused on identifying exposed vulnerabilities prior to their exploitation, and due to timing and urgency considerations, they usually make no attempt at stealth, which may sometimes trigger technical controls that an attacker, using more conservative tactics, might not. Should this occur, remove network blocks and let the scanning service know that their scans were blocked as well as that you have corrected it so they can jumpstart scanning on the particular IPs again, if necessary.
- Include internet-accessible applications in your scanning scope even if only available to your organization. The scope should include all of your static, public IP addresses that are managed by or on behalf of your organization. Do not include private IPs from systems accessible only through your organization's intranet.
- CISA offers a no-cost service comprising vulnerability scanning of static IPv4 IP addresses to identify vulnerabilities on Internet-accessible systems. SLTT governments and private entities should consider taking advantage of this service in addition to periodic tests conducted by network administrators.
- Non-federal organizations can opt to participate in the CISA vulnerability scanning program by sending a request to ncats_info@hq.dhs.gov.

Resource Considerations

- Establishing a vulnerability coordination POC and aligning resources to address identified vulnerabilities detected on Internet-accessible systems is only the beginning and most inexpensive aspect of vulnerability management.
- The next step is implementing a vulnerability and configuration management program to enforce consistent patch management across all hosts within the network environment. This should start with those systems that have critical or prioritized vulnerabilities discovered in the vulnerability scan. When possible, remove end-of-life products from the network.

HELPFUL LINKS AND REFERENCE MATERIALS

CISA Binding Operational Directive 19-02 – Vulnerability Remediation Requirements for Internet-Accessible Systems and FAQ:
https://cyber.dhs.gov/bod/19-02/

CISA Blog Post on BOD 19-02:
https://www.dhs.gov/cisa/blog/2019/04/29/cisa-releases-binding-operational-directive-new-requirements-remediating

For guidance on Enterprise Patch Management Technologies, organizations should consult National Institute of Standards and Technologies (NIST) Special Publication 800-40 Rev. 3 Guide to Enterprise Patch Management Technologies:
https://csrc.nist.gov/publications/detail/sp/800-40/rev-3/final