Appalachian Regional Commission

Evaluation Report

Table of Contents

Results of Evaluation **1**

Problem Areas **2**

Problem Area 1: The Commission's system did not fully measure patching status..... 2

Problem Area 2: The Commission's automated process did not fully patch all systems. 3

Management Comments and Our Analysis **4**

Objective, Scope and Methodology **4**

Results of Evaluation

The purpose of this evaluation was to answer the question:

> Has the ARC implemented an effective, comprehensive system maintaining patch levels?

No. While the ARC did have a process in place to apply patches, the existing process was not fully effective.

The process for patching ARC systems is ineffective and exposes the Commission's information and systems to significant risk. On June 28, 2013 we reviewed the patch status of 45 machines and found that:

- All but five systems were missing High or Critical Severity patches—a High Severity patch is a software change designed to prevent intruders from being able to run code of their choice on the network or elevating their privileges to take control of Commission systems.
- 1258 High or Critical Severity patches were missing on Commission systems.
- An average of 28 High or Critical Severity patches were missing from each system.
- 18 systems (40%) were missing patches that had been released one year ago or prior.
- An average of 19 High or Critical severity patches for third-party (non-Microsoft) software were missing from each system.

When software vendors identify problems with their applications or operating systems, they create and release updates to the software to resolves these issues. These updates are known as 'patches.' These patches are made available to the public, who install these patches to rectify the problems they are intended to solve.

The majority of patches released today are designed to correct previously-identified security flaws. Systems without these patches are vulnerable to these exploits, which could result in an intrusion by malicious individuals. Vulnerabilities defined as High or Critical severity identify those with the highest risk to the systems in question. Once a patch is released, the risk increases for unpatched systems, because it has been publically announced that a flaw is present, and the software patch can be analyzed to precisely identify the nature of the security flaw. Malicious parties use this information to create new exploits if they aren't available already.

In order to manage and reduce the risk to the organization, those responsible for managing its systems must continually track the patched status of those systems, and deploy patches as soon as they are made available. If systems are allowed to remain

unpatched, the ease with which they can be attacked can nullify all other security measures in place at the organization. Patching systems is a primary means of securing systems, and despite potential assertions to the contrary, there are no effective substitutes for this basic security measure. Every unpatched system that connects to the Internet increases the risk to the organization.

The patching process for ARC systems was ineffective because the Commission did not measure its patch status, and it did not have an automated process to fully patch all systems. These problem areas will be discussed in detail in the rest of this report.

Problem Areas

Problem Area 1:
The Commission's system did not fully measure patching status.

The Commission did not measure the patching status of its systems. This lack of monitoring was partially responsible for the fact that systems were not patched. Our analysis of 45 workstations determined that High or Critical severity patches were missing from 40, or 89% of all systems tested. On average, each system was missing 28 High or Critical severity patches.

Effective management is only possible with consistent measurement. Because the Commission did not monitor the patch status of its systems, it could not manage the patching process, or by extension, the security of its network.

Systems with missing patches expose more than just a single computer to risk, but instead they expose all data and systems on the network to risk. An exploited system serves as the entry point into the network for an attacker. Once a foothold is gained, attackers can explore and potentially exploit all systems on that network. One weak link effectively circumvents the other security applied to the network perimeter or the application itself.

In order to execute the mission of the Commission, senior management must remain informed of risks to their underlying systems. Because they were not regularly informed with an accurate picture of the Commission's information security status, they were not aware of the risks to the confidentiality, integrity, and availability of Commission data and systems.

Recommendation 1: Implement a specialized software tool to scan the patch status of all Commission equipment at least weekly. This tool should be distinct from the tool used to patch systems.

Recommendation 2: Report patching status monthly to Commission executive management.

Problem Area 2:
The Commission's automated process did not fully patch all systems.

As of June 28, 2013, the Commission was missing 1258 High or Critical patches on its systems. Due to the sheer number of patches released and the labor required to manually apply them, it is impossible to rely on manual processes to apply patches in a timely manner, and any process that is unable to automatically patch third-party software in insufficient to protect the Commission's data. While Microsoft provides robust, free tools to apply patches to its own software, on its own this software is unable to provide automated patching for third-party software. Third-party software includes common items such as Mozilla Firefox, Adobe Acrobat, and Oracle Java. Of the 45 systems analyzed, 40 were missing High or Critical patches for third-party software. On average, each system was missing 19 patches for third-party software. Attacks of vulnerable third-party software are one of the primary vectors of intrusion.

High or Critical severity patches for all software should be applied Commission-wide within days of release by their manufacturer. To achieve the best protection, these patches should be installed for most systems on the same day a patch is released, because exploits are generated quickly from the information provided as part of the patch. Any delay beyond the release date of a patch increases the risk exposure. For this reason, Microsoft preconfigures Windows operating systems to download and install available patches every night.

Commission staff should be protected from malicious content encountered while browsing the Internet or received via email. Unpatched systems are missing this basic level of protection, and greatly increase the risk of system-wide compromise. Even new builds of systems will be missing patches, and should be fully patched before being brought online.

The Commission's current patching method demands significant resources because it is not fully automated. Because it does not immediately apply all necessary High or Critical severity patches, the Commission is operating under a high level of risk. As a

result, the Commission does not have the most basic level defense to secure its systems and its network. The current patching process does not effectively protect the Commission's information or systems.

Recommendation 3: Implement a specialized software tool to automatically patch all Commission systems.

Recommendation 4: Patch all vulnerable software on all systems.

Recommendation 5: Apply all High or Critical severity patches on the day of release.

Recommendation 6: Fully patch all new systems as part of the build process.

Management Comments and Our Analysis

On July 26th, 2013, management provided comments on the draft evaluation report. They concurred with our assessment that there are two problem areas that resulted in the absence of an effective, comprehensive system maintaining patch levels. They subsequently provided management decisions that would address each of the six recommendations.

At the time of the final report, the Commission had purchased and deployed new tools to improve its ability to fully patch all of its systems in a timely fashion.

Objective, Scope and Methodology

Objective:

Has the ARC implemented an effective, comprehensive system maintaining patch levels?

Scope:

The scope of this evaluation included all servers, workstations, and other network equipment providing services and security on ARC network.

Methodology:

1. Used Nessus with current definitions to perform an authenticated scan of all infrastructure and endpoints related to the ARC network.
2. Identified systems that could not be scanned due to technical or policy issues, and identified a means of configuring these systems so they could be scanned.
3. Analyze vulnerabilities to remove false positives, and classify findings to identify trends and the causes of unpatched vulnerabilities.