Cyber Hygiene Assessment

SC State Election Commission

November 15, 2016
For Official Use Only (FOUO)

Contents

1 How To Use This Report 4

2 Report Card 5

3 Executive Summary 6

4 Methodology 9
   4.1 Background ................................................................. 9
   4.2 Process ................................................................. 9

5 Approximate Host Locations 12

6 Vulnerability Scan Results 13

7 Results Trending 15

8 Conclusion 18

Appendices 19

Appendix A  Vulnerability Summary 19

Appendix B  Vulnerability Changes Since Last Report 20
   B.1 Mitigated Vulnerabilities ............................................. 20
   B.2 New Vulnerabilities Detected ................................. 20
   B.3 Re-Detected (Previously-Mitigated) Vulnerabilities .... 20
   B.4 Recently-Detected Vulnerabilities .......................... 21

Appendix C  Detailed Findings and Recommended Mitigations by Vulnerability 22

Appendix D  Critical and High Vulnerability Mitigations by IP Address 23

Appendix E  False Positive Findings 24

Appendix F  Frequently Asked Questions 25

Appendix G  Attachments 27
List of Figures

1. Top Vulnerabilities by Occurrence ................................................. 6
2. Top High-Risk Hosts .................................................................... 6
3. Top Risk Based Vulnerabilities ....................................................... 6
4. Median Time in Days to Mitigate Vulnerabilities ............................. 7
5. Median Age in Days of Active Vulnerabilities ................................. 7
6. Critical Vulnerability Age Over Time .............................................. 8
7. Active Critical Vulnerability Age ..................................................... 8
8. Approximate Host Locations .......................................................... 12
9. Vulnerability Count per Host ......................................................... 13
10. CVSS Histogram for Active Vulnerabilities ................................. 13
11. Total Active Vulnerabilities Over Time ......................................... 15
12. Active Critical and High Vulnerabilities Over Time ...................... 15
13. Active Medium and Low Vulnerabilities Over Time .................... 15
14. Vulnerable Hosts Over Time ........................................................ 16
15. Distinct Services Over Time .......................................................... 16
16. Distinct Vulnerabilities Over Time ................................................. 16

List of Tables

1. Number of Vulnerabilities by Severity Level .................................. 6
2. Top Operating Systems Detected .................................................... 7
3. Top Services Detected ................................................................... 7
4. Active Critical Vulnerability Age Summary .................................. 8
5. Number of Vulnerabilities by Severity Level .................................. 8
6. Top Vulnerabilities by Common Vulnerability Scoring System (CVSS) 13
7. Top Hosts by Weighted Risk ........................................................ 14
8. Risk Rating System ..................................................................... 14
9. Comparison with Previous Report ................................................. 17
1  How To Use This Report

Welcome to your Cyber Hygiene (CyHy) report. This document aims to be a comprehensive weekly snapshot of known vulnerabilities detected on Internet-facing hosts for SC State Election Commission (SEC).

You may wonder what you’re supposed to do with all this information. While it’s not our intent to prescribe to you a particular process for remediating vulnerabilities, we hope you’ll use this report to strengthen your security posture. Here’s a basic flow:

1. Review the Cyber Hygiene Report Card for a high-level overview. This section gives a quick comparison of the problems we find week to week. If this is your first report, you should note that the Report Card will initially lack historical data to make comparisons against, though that data will exist in your next report.

2. See Appendix A: Vulnerability Summary for a list of unique vulnerabilities across all the systems we detect problems with. Appendix C: Detailed Findings and Recommended Mitigations by Vulnerability provides more information about each vulnerability and all the hosts that we detect are susceptible to a given vulnerability. You should focus on those vulnerabilities rated with the greatest severity, as well as those that impact your high-value assets, but don’t ignore the medium or low vulnerabilities. Recognize that a vulnerability’s rating tends to get worse with time.

3. If this report is not your first, review Appendix B: Vulnerability Changes Since Last Report for a breakdown of all the changes we detected in your scope in the last week.

4. If you’ve patched a vulnerability since your last report, verify it’s listed here. If it’s not present, there may still be an issue. It may also be possible that the fix was done after our latest scan, which was on November 15, 2016.

5. For additional analysis, see Appendix G: Attachments, which provides Comma-Separated Values (CSV) files for all findings, services, hosts, and the scope that we scan.

You should be aware that Cyber Hygiene does not scan your entire scope every week, but does attempt to scan every host each week. For an explanation of how CyHy works, see the Methodology section.

As you review the report, you may have additional questions. Check out the answers we provide in the Frequently Asked Questions section. If you have any additional questions, email us at ncatshq.dhs.gov.
# CYBER HYGIENE REPORT CARD

## High Level Findings

<table>
<thead>
<tr>
<th>Addresses Owned</th>
<th>Addresses Scanned</th>
<th>Latest Scans</th>
</tr>
</thead>
<tbody>
<tr>
<td>64 ✈️ no change</td>
<td>64 ✈️ no change</td>
<td>Addresses: September 12, 2016 – November 15, 2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vulnerabilities: November 8, 2016 – November 15, 2016</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hosts</th>
<th>Vulnerable Hosts</th>
<th>Vulnerabilities</th>
<th>Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 ✈️ no change</td>
<td>1 ✈️ no change</td>
<td>1 ✈️ no change</td>
<td>10 ✈️ no change</td>
</tr>
<tr>
<td></td>
<td>50% of hosts vulnerable</td>
<td>no change</td>
<td>no change</td>
</tr>
</tbody>
</table>

## Vulnerabilities

<table>
<thead>
<tr>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 ✈️</td>
<td>0 ✈️</td>
<td>0 ✈️</td>
<td>1 ✈️</td>
</tr>
<tr>
<td>0 resolved</td>
<td>0 resolved</td>
<td>0 resolved</td>
<td>0 resolved</td>
</tr>
<tr>
<td>0 new</td>
<td>0 new</td>
<td>0 new</td>
<td>0 new</td>
</tr>
</tbody>
</table>

## Vulnerability Response Time (since September 12, 2016)

<table>
<thead>
<tr>
<th>Days to Mitigate</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median</td>
<td>25</td>
<td>25</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>Maximum</td>
<td>25</td>
<td>25</td>
<td>52</td>
<td>52</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Days Currently Active</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Median</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
</tr>
<tr>
<td>Maximum</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
</tr>
</tbody>
</table>
3 Executive Summary

This report provides the results of a Department of Homeland Security (DHS) / National Cybersecurity Assessments and Technical Services (NCATS) CyHy assessment of SEC conducted from September 12, 2016 at 18:09 UTC through November 15, 2016 at 20:01 UTC. The Cyber Hygiene assessment includes network mapping and vulnerability scanning for Internet-accessible SEC hosts. This report is intended to provide SEC with enhanced understanding of their cyber posture and to promote a secure and resilient Information Technology (IT) infrastructure across SEC’s Internet-accessible networks and hosts.

For this reporting period, a total of 2 hosts were identified out of the 64 addresses provided to NCATS. The scanning revealed 1 total potential vulnerabilities on 1 vulnerable hosts, 50% of all SEC hosts. 9 distinct open ports, 4 distinct services, and 4 operating systems were detected.

1 distinct types of potential vulnerabilities (0 critical, 0 high, 0 medium, and 1 low) were detected, as shown in Table 1. The vulnerabilities that were detected most-frequently on SEC hosts are displayed in Figure 1.

SEC should review the vulnerabilities detected and report any false positives back to NCATS so they can be excluded from future reports. Please refer to Appendix A: Vulnerability Summary for an illustration of the breakdown of vulnerability occurrences over time.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Distinct Vulnerabilities</th>
<th>Total Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>0% 0</td>
<td>0% 0</td>
</tr>
<tr>
<td>High</td>
<td>0% 0</td>
<td>0% 0</td>
</tr>
<tr>
<td>Medium</td>
<td>0% 0</td>
<td>0% 0</td>
</tr>
<tr>
<td>Low</td>
<td>100% 1</td>
<td>100% 1</td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 1: Number of Vulnerabilities by Severity Level

Figure 1: Top Vulnerabilities by Occurrence

Additionally, the top high-risk hosts and top risk based vulnerabilities are displayed in Figure 2 and Figure 3. For more information about these risk calculations, refer to Table 8: Risk Rating System.

Figure 2: Top High-Risk Hosts

Figure 3: Top Risk Based Vulnerabilities
The most frequently detected operating systems and services for SEC are displayed in Table 2 and Table 3 respectively.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>91.7%</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2.8%</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>2.8%</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 2: Top Operating Systems Detected

<table>
<thead>
<tr>
<th>Service</th>
<th>60.0%</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>20.0%</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>10.0%</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 3: Top Services Detected

The next two figures illustrate how quickly SEC responds to vulnerabilities that have been identified. Figure 4 shows how long it has taken SEC to mitigate vulnerabilities of each severity level (for vulnerabilities mitigated since September 12, 2016), while Figure 5 shows the median ages of current active vulnerabilities. Vulnerability age is based on the initial detection date by CyHy.

![Figure 4: Median Time in Days to Mitigate Vulnerabilities](image)

![Figure 5: Median Age in Days of Active Vulnerabilities](image)
Figure 6 displays the number of active critical vulnerabilities that were less than 30 days old and more than 30 days old, as of the date indicated on the graph. Vulnerability age is based on the initial detection date by CyHy.

![Critical Vulnerability Age Over Time](image)

Figure 6: Critical Vulnerability Age Over Time

Figure 7 and Table 4 provide an age breakdown of every currently active critical vulnerability for SBC.

**No Critical Vulnerabilities Detected**

**Figure Omitted**

![Active Critical Vulnerability Age](image)

<table>
<thead>
<tr>
<th>Days</th>
<th>0-7</th>
<th>7-14</th>
<th>14-21</th>
<th>21-30</th>
<th>30-90</th>
<th>90+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Critical Vulnerabilities</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 4: Active Critical Vulnerability Age Summary
4 Methodology

4.1 Background

The NCATS team conducted a Cyber Hygiene assessment of SEC’s Internet-facing networks and hosts from September 12, 2016 at 18:09 UTC through November 15, 2016 at 20:01 UTC. This report provides result summaries and detailed findings of the CyHy assessment activity for SEC. All scan results are included in Appendix G: Attachments as CSV files.

Cyber Hygiene is intended to improve your security posture by proactively identifying and reporting on vulnerabilities and configuration issues present on Internet-facing systems before those vulnerabilities can be exploited.

Cyber Hygiene is a service of NCATS, organized under the DHS National Protection and Programs Directorate (NPPD), Office of Cybersecurity and Communications (CS&C), National Cybersecurity and Communications Integration Center (NCCIC), NCCIC Operations and Integration (NO&I).

DHS began Cyber Hygiene in January 2012 to assess, on a recurring basis, the “health” of unclassified federal civilian networks accessible via the Internet. Since then, the program has grown to provide a persistent scanning service to federal, state, local, tribal, and territorial governments and private sector organizations.

Upon submission of an Acceptance Letter, SEC provided NCATS with their public network address information. SEC and NCATS agreed on any time restrictions which would be imposed on the scanning activity.

4.2 Process

All Cyber Hygiene scanning activity originates from the 64.69.57.0/24 network.

CyHy uses a combination of scanning services for testing:

- Network Mapping
- Vulnerability Scanning

Network Mapping

Using Nmap, we attempt to determine what hosts are available, identify what services (application name and version) those hosts are offering, and what Operating System (OS) versions they are running. We first scan the most-commonly-detected 1,000 Transmission Control Protocol (TCP) ports of the addresses you’ve submitted to us to get a quick understanding of the active/dark landscape. An address that has at least one port open/listening service is considered a 'host' and is then fully port-scanned (TCP) and included in the vulnerability scan.

If no services are detected in the most common 1,000 ports on a given Internet Protocol (IP) address, that address is labelled 'dark' in CyHy and will be re-scanned after at least 90 days to check for change. Addresses marked dark are not included in the host count of the weekly report. Understand that CyHy is not attempting to make a judgment call about why an address is unresponsive. If there’s not a port open, it’s not a ‘host’ in the language of CyHy.

Vulnerability Scanning

Using Nessus, each host is evaluated against a library of vulnerabilities that an Internet-based actor could exploit. Vulnerabilities are reported with a severity of critical, high, medium, or low to facilitate prioritization of remediation efforts. We enable all Nessus Plugins [https://www.tenable.com/plugins/] except the ones in the 'Denial of Service' family.
Scanning Frequency

Scanning occurs continuously between each weekly report. All hosts are scanned for vulnerabilities at least once a week; hosts with vulnerabilities are scanned more frequently.

Cyber Hygiene’s scan prioritization is as follows:

- Addresses with no running services detected (dark space) are rescanned after at least 180 days.
- Hosts with no vulnerabilities detected are rescanned every 14 days.
- Hosts with low-severity vulnerabilities are rescanned every 12 days.
- Hosts with medium-severity vulnerabilities are rescanned every 8 days.
- Hosts with high-severity vulnerabilities are rescanned every 2 days.
- Hosts with critical-severity vulnerabilities are rescanned every 24 hours.

You should understand that a single host may have multiple vulnerabilities of varying severity, which impacts the frequency that single host is scanned.

To be clear, it is not the case that we scan your entire address scope for vulnerabilities each week (unless each address you’ve provided to us has a responsive host). It is the case, though, that each host will get vulnerability scanned at least once per week.

Recurring Vulnerabilities

After you’ve remediated a vulnerability (and it remains resolved for a period of 90 days), the host’s scan priority will drop. This approach allows the NCATS team to focus on the areas of importance and give more attention to the hosts that need it.

Vulnerabilities are assigned an age in order to track timeliness of remediation. Vulnerability age is determined by when it was first detected on a host, not from when it first appeared on a report. As scanning occurs continuously between weekly reports, it is possible to have “new” vulnerabilities appear on a report that are already days old. It is also possible for a vulnerability to fluctuate between being ‘detected’ and ‘not detected’ during mid-week scans and then at a future time appear in a report as many days old. If a mitigated vulnerability is re-detected less than 90 days after the date of non-detection, it will be considered to be the same vulnerability with the same ‘initial detection date’ as previously recorded. If it is re-detected more than 90 days after the date of non-detection, it will be treated as a new vulnerability with a new ‘initial detection date’.

Vulnerability Scoring

The Nessus vulnerability scanner references the National Vulnerability Database (NVD) [https://nvd.nist.gov/] for its vulnerability information. The NVD provides CVSS scores for many known vulnerabilities. In particular, NVD supports the CVSS version standard for all Common Vulnerabilities and Exposures (CVE) vulnerabilities.

The CVSS is a free and open industry standard for assessing the severity of computer system security vulnerabilities. CVSS attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat. The NVD uses severity rankings of “Low,” “Medium,” and “High” in addition to the numeric CVSS scores, but these qualitative rankings are simply mapped from the numeric CVSS base scores:

- Vulnerabilities are labeled “Low” severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-10.0.

Nessus has a “critical” rating which it uses for CVSS 10 vulnerabilities. Where the NVD has not provided a CVE severity rating, the Nessus scanner relies on its own rankings.
What's In The Report?

Though Cyber Hygiene initiates multiple scans between reports, only the latest scan data for each host is used to determine current vulnerability. This is the data that appears in the main body of the report and in Appendix A: Vulnerability Summary, Appendix B.2: New Vulnerabilities Detected and Appendix B.3: Re-Detected (Previously-Mitigated) Vulnerabilities.

If a vulnerability was detected since that last report (e.g., it wasn’t in the previous report’s findings, though CyHy saw it mid-week) but it was not in the latest scan, we include it in Appendix B.4: Recently-Detected Vulnerabilities.

If a vulnerability that was previously reported to you is no longer detected by the latest scan, the vulnerability and host will be listed in Appendix B.1: Mitigated Vulnerabilities.

We encourage you to validate the status of vulnerabilities in both Appendix B.1: Mitigated Vulnerabilities and Appendix B.4: Recently-Detected Vulnerabilities against your change control register. This will help to ensure that the vulnerability we detected has actually been remediated and is not simply unresponsive to our scans.
5  Approximate Host Locations

The map below shows the approximate locations of detected hosts as listed in a geo-location database. This map is provided as a tool to identify hosts that may have been mistakenly added to, or removed from scope. The map is scaled to include all known SEC host locations.

Figure 8: Approximate Host Locations
6 Vulnerability Scan Results

For this period, CyHy detected 1 occurrences of 1 distinct vulnerabilities (0 critical, 0 high, 0 medium, and 1 low). SEC should review the vulnerabilities detected and report any false positives back to NCATS so these can be excluded from future reports (see the Frequently Asked Questions section for more about false positives).

The scanning detected 1 vulnerable hosts — 1 hosts with one to five vulnerabilities were identified; 0 hosts had between six and nine vulnerabilities; 0 hosts had ten or more vulnerabilities identified.

<table>
<thead>
<tr>
<th>Severity</th>
<th>Distinct Vulnerabilities</th>
<th>Total Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>High</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Medium</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Low</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Table 5: Number of Vulnerabilities by Severity Level

The CVSS scores for all active vulnerabilities can be found in Figure 10.

![Figure 10: CVSS Histogram for Active Vulnerabilities](image)

The top vulnerabilities according to CVSS score are represented in Table 6.

<table>
<thead>
<tr>
<th>Vulnerability Name</th>
<th>Severity</th>
<th>Hosts</th>
<th>CVSS Score</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>1</td>
<td>2.6</td>
</tr>
</tbody>
</table>

Table 6: Top Vulnerabilities by CVSS
A complete list of distinct vulnerabilities detected, including severity level and number of hosts having the vulnerability can be found in Appendix A: Vulnerability Summary. Full details on every detected vulnerability can be found in Appendix C: Detailed Findings and Recommended Mitigations by Vulnerability. Every critical and high finding detected, along with the hosts that have these findings, are listed in Appendix D: Critical and High Vulnerability Mitigations by IP Address.

The top high-risk hosts are identified in Table 7 by combining the total number of vulnerabilities, the severity of the vulnerabilities, and a weighted CVSS score for vulnerabilities detected. For more information on the formula, please refer to Table 8: Risk Rating System.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Critical</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 7: Top Hosts by Weighted Risk

The Risk Rating System (RRS) emphasizes higher-rated CVSS scores to ensure that hosts with a large number of lower-risk vulnerabilities do not outweigh hosts with a smaller number of high-risk vulnerabilities, while ensuring that hosts with an extreme number of low-risk vulnerabilities are not overshadowed by hosts with a single higher-risk issue. The RRS also ensures that hosts with a significant number of high-risk vulnerabilities will not be overshadowed by a host with only a single critical vulnerability.

Table 8 illustrates the base and weighted CVSS scores and shows the equivalent number of lower-risk vulnerabilities to weigh evenly with a single critical (CVSS score of 10) vulnerability.

<table>
<thead>
<tr>
<th>Base CVSS Score</th>
<th>Weighted CVSS Score</th>
<th>Equivalent to CVSS Score 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>$1 \times 10^{-06}$</td>
<td>10,000,000.0</td>
</tr>
<tr>
<td>2.0</td>
<td>0.000,128</td>
<td>78,125.0</td>
</tr>
<tr>
<td>3.0</td>
<td>0.002,187</td>
<td>4,572.47</td>
</tr>
<tr>
<td>4.0</td>
<td>0.016,384</td>
<td>610.35</td>
</tr>
<tr>
<td>5.0</td>
<td>0.078,125</td>
<td>128.0</td>
</tr>
<tr>
<td>6.0</td>
<td>0.279,936</td>
<td>35.72</td>
</tr>
<tr>
<td>7.0</td>
<td>0.823,543</td>
<td>12.14</td>
</tr>
<tr>
<td>8.0</td>
<td>2.097,152</td>
<td>4.77</td>
</tr>
<tr>
<td>9.0</td>
<td>4.782,969</td>
<td>2.09</td>
</tr>
<tr>
<td>10.0</td>
<td>10.0</td>
<td>1.0</td>
</tr>
</tbody>
</table>

Table 8: Risk Rating System

As an example, a host having 400 vulnerabilities with a base CVSS score of 1.0 would get a weighted RRS score of $4 \times 10^{-04}$, which is considered lower-risk than a host with a single critical vulnerability (RRS score of 10.0). Similarly, a host having 4 vulnerabilities with a base CVSS score of 8 would get a RRS score of 8.39 and still be considered a lower risk than a host with a single critical vulnerability (RRS score of 10.0).
7 Results Trending

To help decision-makers, this section provides a comparison of the current data against similar CyHy scans conducted over time.
SEC vulnerability profile over time, reporting on the total hosts detected, number of hosts with vulnerabilities, number of distinct services, and the number of distinct vulnerabilities detected can be found in Figure 14, Figure 15, and Figure 16 respectively.
<table>
<thead>
<tr>
<th></th>
<th>Previous Report</th>
<th>Current Report</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>2</td>
<td>2</td>
<td>0.0%</td>
</tr>
<tr>
<td>Vulnerable Hosts</td>
<td>1</td>
<td>1</td>
<td>0.0%</td>
</tr>
<tr>
<td>Distinct Services</td>
<td>4</td>
<td>4</td>
<td>0.0%</td>
</tr>
<tr>
<td>Distinct Vulnerabilities</td>
<td>1</td>
<td>1</td>
<td>0.0%</td>
</tr>
<tr>
<td>Distinct Operating Systems</td>
<td>4</td>
<td>4</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

Table 9: Comparison with Previous Report

Overall, for all hosts identified, SEC averaged 0.5 vulnerabilities per host. For vulnerable hosts, SEC averaged 1.0 total vulnerabilities per host. By severity, vulnerable hosts averaged 0.0 critical, 0.0 high, 0.0 medium, and 1.0 low vulnerabilities per host.
8 Conclusion

The results and data contained in this report are provided for SEC, and should be used to correct any identified vulnerabilities, configuration errors, and security concerns in SEC’s external network perimeter. The CyHy service seeks to improve the cybersecurity posture of NCATS’ stakeholders by maintaining tactical awareness of the operational awareness and cyber health of individual organizations. Additionally, NCATS will provide a non-attributable overview of all collected data detailing trends and analysis at the end of the fiscal year. If SEC has questions, comments, or concerns about the findings or data contained in this report, please work with your designated technical point of contact when requesting assistance from NCATS at ncatshq.dhs.gov.
Appendix A  Vulnerability Summary

This section presents counts of all distinct vulnerabilities that were detected in the latest scans. It shows the name of the vulnerability, the severity level of the vulnerability and the number of vulnerability detections in the previous report vs. this report. Low, medium, high, and critical vulnerabilities are displayed.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Severity</th>
<th>Previous</th>
<th>Current</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>1</td>
<td>1</td>
<td>0.0%</td>
</tr>
</tbody>
</table>
Appendix B  Vulnerability Changes Since Last Report

B.1 Mitigated Vulnerabilities

This section lists the vulnerabilities that were included on the previous report, but were not detected by the latest scans. The initial detection and mitigation detection dates are provided, plus the number of days it took to mitigate each vulnerability.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Severity</th>
<th>Host</th>
<th>Port</th>
<th>Initial Detection</th>
<th>Mitigation Detected (UTC)</th>
<th>Days To Mitigate</th>
</tr>
</thead>
</table>

There were no vulnerabilities mitigated since the previous report.

B.2 New Vulnerabilities Detected

This section lists the new vulnerabilities that were detected for the first time in the latest scans. The initial detection and latest detection dates are provided for each vulnerability.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Severity</th>
<th>Host</th>
<th>Port</th>
<th>Initial Detection (UTC)</th>
<th>Latest Detection (UTC)</th>
</tr>
</thead>
</table>

There were no new vulnerabilities detected for the first time by the latest scans.

B.3 Re-Detected (Previously-Mitigated) Vulnerabilities

This section lists the vulnerabilities that were previously detected, then mitigated, and were re-detected in the latest scans. The initial detection and latest detection dates are provided for each vulnerability.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Severity</th>
<th>Host</th>
<th>Port</th>
<th>Initial Detection (UTC)</th>
<th>Latest Detection (UTC)</th>
<th>Age Days</th>
</tr>
</thead>
</table>

There were no previously-mitigated vulnerabilities that were re-detected.
B.4 Recently-Detected Vulnerabilities

This section lists the vulnerabilities that were detected since the last report, but not detected in the latest scans. The initial detection and latest detection dates are provided for each vulnerability. It is strongly recommended to verify if the vulnerabilities below were actively mitigated by your organization. If they were not, it is highly likely these vulnerabilities will be detected again by future scans.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Severity</th>
<th>Host</th>
<th>Port</th>
<th>Initial Detection (UTC)</th>
<th>Latest Detection (UTC)</th>
<th>Age Days</th>
</tr>
</thead>
</table>

There were no recently-detected vulnerabilities that were not detected in the latest scans.
Appendix C  Detailed Findings and Recommended Mitigations by Vulnerability

This section presents detailed scan results from the network mapping and vulnerability scans. Vulnerabilities identified have a recommended mitigation solution that should be considered in order to establish or maintain a secure network.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Severity</th>
<th>CVSS</th>
<th>Solution</th>
<th>Affected Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Low</td>
<td>2.6</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Initial Detection: 2016-11-03 18:47 UTC
Latest Detection: 2016-11-15 20:01 UTC
Description: TBD
Appendix D  Critical and High Vulnerability Mitigations by IP Address

This section presents detailed scan results, ordered by host, from the network mapping and vulnerability scans. Only high and critical vulnerabilities are displayed. Vulnerabilities identified have a recommended mitigation solution that should be considered in order to establish or maintain a secure network.

<table>
<thead>
<tr>
<th>Host</th>
<th>Port(s)</th>
<th>Vulnerability</th>
<th>Severity</th>
<th>Age</th>
<th>Solution</th>
</tr>
</thead>
</table>

There were no critical or high vulnerabilities detected.
Appendix E  False Positive Findings

This section lists findings that SEC asserted to NCATS to be false positive (i.e. data that incorrectly indicates a vulnerability is present). If SEC would like to report findings for false positive consideration, please submit an email through your designated technical point of contact with an analysis and evidence indicating how SEC determined the finding is a false positive. Unless NCATS determines the submission is insufficient, NCATS will leave the determination for what constitutes a false positive to report recipients. False positive status expires by default 365 days after the false positive was marked as such by NCATS. When a finding’s false positive status expires, the finding will be removed from this section. If the finding is then re-detected, its status should be reviewed.

<table>
<thead>
<tr>
<th>Vulnerability</th>
<th>Severity</th>
<th>Host</th>
<th>Port</th>
<th>Initial Detection (UTC)</th>
<th>Latest Detection (UTC)</th>
<th>False Positive Effective</th>
<th>False Positive Expiration</th>
</tr>
</thead>
</table>

There are currently no false positive findings.
Appendix F  Frequently Asked Questions

This section seeks to answer the most frequently asked questions about Cyber Hygiene reports.

1. "I think the vulnerability listed in my report is a false positive. Can you remove it from my report?"
   - If you believe a finding to be in error, you can submit a false positive assertion to ncats@hq.dhs.gov which should include the following:
     - The name of the vulnerability
     - IP address and port
     - Your analysis and supporting evidence
   NCATS will review and perform our own analysis. This will not include exploiting a vulnerability, but may include actively sending packets to the host in question.
   - If our research appears to confirm your analysis, the vulnerability will be marked as a false positive for that host and will stop appearing in the main body of report for 1 year. Vulnerabilities marked as 'false positive' will be reported in Appendix E: False Positive Findings, along with the name and date of the individual who submitted the request to us.
   - NCATS reserves the right to assert that certain findings are not false positives, and when false positive assertions are accepted by NCATS, that acceptance should not be construed as validation that a finding is in fact a false positive.

2. "Can I get the data you created this report from in CSV?"
   - Certainly! See Appendix G: Attachments.

3. "I fixed a vulnerability listed in my report. Can you rescan to verify?"
   - CyHy automatically rescans whenever a vulnerability is detected, so there is no need to notify us that you’ve fixed something. If we can no longer detect the vulnerability, it will be listed in Appendix B.1: Mitigated Vulnerabilities.

4. "Can I add my third-party hosted/managed servers?"
   - Yes, and we recommend that you do so, but we request that you obtain authorization/consent before we begin scanning them. DHS does not require documentation from your third-parties.

5. "Why do the host counts in my Cyber Hygiene report not match the number of known Internet-facing end points on my network?"
   - This is likely due to a difference in what we’re defining as a host. CyHy considers a device a host if there is at least one open port/service operating at the address. When we scan, any number of things can occur that make it appear that nothing is at that address (e.g., our scans are blocked by host or network filters, the device is down for maintenance, packets are dropped or lost en route, etc.).
   - The intent of CyHy is to find vulnerabilities, not count hosts, and our metrics should not be relied upon as a verified host count of your organization. The weekly hosts count should be taken as an estimate. If, however, there are no or extremely low host counts reported when there are known active hosts, it is possible that the CyHy scans are being blocked.

6. "I’ve added a new host and your scans are not picking it up."
   - CyHy is not scanning your entire IP scope every week. If you’ve stood up a new server in a range that we only recently scanned and found nothing in, it’s possible that the new server would not appear for nearly 90 days. If you want the new host to be scanned immediately, you can email ncats@hq.dhs.gov and we’ll manually scan it, which will add it to your weekly report.

7. "I’m getting SSL/TLS certificate vulnerabilities that I think are incorrect."

• In our scans, we will use the Mozilla trust store. NCATS will not accept any other roots. This is done as a matter of practice and principle: as practice, because maintaining private roots from our various stakeholders is operationally infeasible; as principle, because our scans aim to ensure that the user of your services is protected. The Mozilla trust store is generally representative of a ‘lowest common denominator’ in what a public-serving site can reasonably expect of those users whose devices they do not manage.

• Ensure that the root your certificate is issued from is included in the Mozilla root store. You should also verify that the intermediate certificates are presented with your site certificate. This allows the scanner to validate the certificate’s chain of trust.

• Though the site is Federal Government-centric, tons of great information can be found at https://cio.gov regarding Hypertext Transfer Protocol Secure (HTTPS), much of which is applicable for SSL/TLS more generally.

8. "Can you scan my IPv6 addresses?"

• There is currently no ETA for CyHy to scan IPv6 addresses.

9. "Can you scan this list of domains for me?"

• For vulnerability scanning, CyHy does not presently scan domain names directly, but we expect to do so in FY17.

10. "How can I change who receives my Cyber Hygiene report?"

• The CyHy report will be delivered to a single address. Most organizations set up a distribution address which takes incoming mail and delivers it to individual mailboxes. NCATS strongly recommends this approach because it allows your organization to grant access to the report to whomever you’d like, as well as manage the change control of employees onboarding or leaving. If you need to change the distro we mail to, email us at ncats@hq.dhs.gov.

11. "Can I change the password for my report?"

• If you need to request a new password for your report, email us at ncats@hq.dhs.gov. Please let us know if you’d like the password texted, delivered over the phone (note if voicemail is ok), or just emailed back.

12. "How is the age of each vulnerability calculated?"

• Vulnerability age is determined by when it was first detected on a host, not from when it first appeared on a report. For more information, refer to the "Recurring Vulnerabilities" paragraph in Section 4.2: Methodology / Process.
Appendix G  Attachments

If your PDF viewer supports embedded attachments you will see paperclip icons below for each attached file.

- **findings.csv**: Detailed list of all vulnerability findings for each IP address and port.
- **recently-detected.csv**: List of all vulnerabilities detected since the last report, but not detected in the latest scans.
- **services.csv**: List of all discovered services and the associated IP address and port.
- **hosts.csv**: List of hosts discovered with IP address, best-guess OS identification, and hostname if available.
- **scope.csv**: List of IP addresses that were in scope for this report.
- **false-positive-findings.csv**: List of all reported false positive vulnerability findings.
Appendix H  Glossary and Acronyms

Glossary

active vulnerability  A vulnerability that was detected in the most recent scan of a host used for this report. 7, 13

false positive  Any normal or expected behavior that is identified in this report as a potentially exploitable vulnerability. 6, 13, 24, 25, 27

host  A device that has at least one open port/listening service. 4, 6, 9, 10, 12–14, 17, 23, 25, 27

initial detection  The initial point in time when Cyber Hygiene scans identified a vulnerability. This date is used to calculate the vulnerability’s age. 7, 8, 10, 20, 21

IP address  A numerical label that identifies each device using the Internet Protocol to communicate over a network. 25

latest detection  The most recent time when Cyber Hygiene scans identified a particular vulnerability. 20, 21

mitigation detection  The date when a previously identified vulnerability was no longer detected by Cyber Hygiene scans. 20

service  An application running at the network application layer that provides communications capabilities across an IP computer network. 4, 9, 10, 16, 27

severity  Please review the following guide for vulnerability severity scoring information: https://www.first.org/cvss/v2/guide. 4, 10, 14, 17, 19

vulnerability  A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. 4, 6–10, 13, 14, 16–25, 27

vulnerability age  The time between a vulnerability’s initial detection date and its latest detection date. 7, 8, 10, 26

vulnerable host  A host with at least one vulnerability detected on the most recent scan used for this report. 17

Acronyms


CSV  Comma-Separated Values. 4, 9, 25

CVE  Common Vulnerabilities and Exposures; for more information refer to https://cve.mitre.org/about/faqs.html. 10

CVSS  Common Vulnerability Scoring System; for more information refer to https://www.first.org/cvss/v2. 3, 10, 13, 14

CyHy  Cyber Hygiene. 4, 6–9, 11, 13, 15, 18, 25, 26

DHS  Department of Homeland Security [https://www.dhs.gov]. 6, 9, 25

HTTPS  Hypertext Transfer Protocol Secure. 26

IP  Internet Protocol. 9, 25, 27
IT  Information Technology. 6

NCATS  National Cybersecurity Assessments and Technical Services. 6, 9, 10, 13, 18, 24–26

NCCIC  National Cybersecurity and Communications Integration Center [https://www.dhs.gov/about-national-cybersecurity-communications-integration-center]. 9

NO&I  NCCIC Operations and Integration. 9

NPPD  National Protection and Programs Directorate [https://www.dhs.gov/national-protection-and-programs-directorate]. 9

NVD  National Vulnerability Database; for more information refer to https://nvd.nist.gov. 10

OS  Operating System. 9, 27

RRS  Risk Rating System. 14

SEC  SC State Election Commission. 4, 6–9, 12, 13, 16–18, 24

TCP  Transmission Control Protocol. 9