National Cybersecurity Assessment and Technical Services (NCATS)

Year-End Engagement Report 2014

Homeland Security

National Cybersecurity and Communications Integration Center

Table of Contents

Welcome from the DHS NCCIC

I am pleased to provide a status update about the ongoing cyber programs and efforts underway at the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC). DHS is responsible for protecting the Nation's critical infrastructure from physical and cyber threats, including those impacting business and government operations, emergency preparedness communications, process control systems and infrastructures. Within DHS's National Protection and Programs Directorate (NPPD), the NCCIC serves as a centralized location to coordinate the national response to cyber incidents, provide shared situational awareness across the Federal Government; state, local, tribal, and territorial governments (SLTT); the private sector; and international entities, and respond to significant cyber events. The NCCIC provides cybersecurity and communications situational awareness to leadership and key decision makers on vulnerabilities, intrusions, incidents, mitigation, and recovery actions.

As cybersecurity threats continue to evolve, our ability to outpace the threat relies in part on integrating proactive services within an increasingly robust suite of capabilities to advance computer network protection and defense. In Fiscal Year 2014 (FY14), the NCCIC operationalized the National Cybersecurity Assessments and Technical Services (NCATS) team, which plays a critical cyber role through the delivery of proactive prevention, protection, and response services to decrease the Nation's overall susceptibility to cyber threats and impacts. It is my privilege to share the NCATS 2014 End-of-Year Report with our stakeholders and provide you with information on how NCATS has advanced over the past year.

We will continue to share reports that reflect our advancements in security and resilience across our cyber environment. I look forward to your feedback.

Regards,

Greg Touhill

Brigadier General, USAF (ret)
Deputy Assistant Secretary for Cybersecurity Operations and Programs
Office of Cybersecurity and Communications
U.S. Department of Homeland Security

NCATS Mission

Over the past few years, the DHS NCATS team significantly enhanced their capabilities to assess the state of operational readiness and the cybersecurity risks to unclassified networks, applications, and systems. Along the way, there were many success stories, lessons learned, and a driven mission to improve cybersecurity. With the move from DHS' Federal Network Resilience to the NCCIC, during FY14, the NCATS team expanded their service scope beyond federal agencies to include organizations representing the Critical Infrastructure sectors. The NCATS team achieved our goals of arming stakeholders with the robust tools and data to mitigate risks; and, delivered policymakers at the highest level a holistic enterprise view of the Federal Government's cybersecurity posture.

The NCATS team found that federal, SLTT, and critical infrastructure entities, regardless of size, scope of work, or mission, face similar information security risks. The most common risks identified by NCATS were outdated systems or applications with known flaws; but serious risks need to be addressed even with new or upgraded systems and applications,. The cybersecurity landscape evolves at a breakneck speed, giving our adversaries the advantage –along with frequent opportunities – to identify and exploit weaknesses. During FY14 the NCATS team responded to support stakeholders during the Heartbleed exposure that proved to be the most significant Internet vulnerability of the year. Due to the rapidly changing security and threat environments, stakeholders face a daunting task to defend and secure all avenues of attack in a constrained budget environment.

As FY14 comes to a close, this report presents a comparison of year to year data. As the NCATS team grows in strength and experience, the quality and depth of this data will only improve. In order to protect the integrity and confidentially of our stakeholders' networks, the data in this report is non-attributable to any federal agency, SLTT, or critical infrastructure entity.

The report is intended to reach government and industry leaders, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), and technical support staff communities. By sharing our conclusions from multiple years of cybersecurity assessments, NCATS can disseminate the most common methods used to compromise systems and facilitate improved risk management across all levels of the government and private sector critical infrastructure. Through this report, the NCATS team hopes readers will be able to identify similarities in their own environment and initiate proactive steps to reduce overall risk to cyber assets.

Regards,

Rob Karas

Chief for the National Cybersecurity Assessments and Technical Services
National Cybersecurity and Communications Integration Center
U.S. Department of Homeland Security

NCATS Report Highlights

Expert Analysis, Actual Data

This second annual NCATS report presents summary non-attributable findings generated using actual data from operational testing and scanning in FY14. This work is performed by NCATS security engineers and analysts to identify vulnerabilities, evaluate risks, and offer prioritized remediation guidance. The proactive risk-based approach used by NCATS provides expert analysis to empower stakeholders to mitigate risks, close capability gaps, limit exposure, reduce exploitation, and increase the speed and effectiveness of cyber-attack response. NCATS analyzes stakeholder systems through its Risk and Vulnerability Assessments (RVA) and Cyber Hygiene (CH) service offerings.

Standardized methods, processes, and procedures are used to collect the data during RVA and CH testing and include both scheduled stakeholder engagements and event-driven testing, such as scanning conducted to determine the prevalence of the Heartbleed vulnerability across the federal government. In this second annual report, a comparison of past years statistics with current information is provided where meaningful. As NCATS is strongly committed to protecting the privacy of its stakeholders, data is only presented as non-attributable aggregate statistics.

FY14 Key Data Highlights

This year's most notable highlights include results from testing and assessments of systems and networks belonging to federal agencies, SLTT governments, and critical infrastructure organizations. As in previous years, these results reveal the importance of including manual testing to identify security issues not detected by vulnerability scanners.

67% …of all RVA findings were identified through **MANUAL** testing

RVA **PHISHING** emails resulted in a click rate of… **25%**

46% …of RVAs resulted in an **EASILY GUESSABLE CREDENTIALS** finding

DNSSEC Compliant Federal .gov **DOMAINS** … **85%**

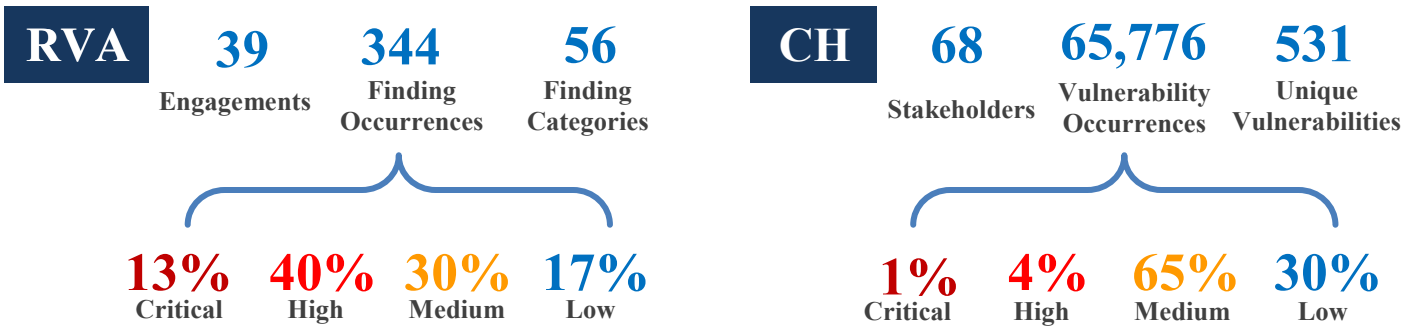
99% …of identified federal **HEARTBLEED** instances were mitigated in three weeks

Patch Management remains the top finding for both RVA and Cyber Hygiene

Cross-site scripting (XSS) is a top RVA web assessment finding

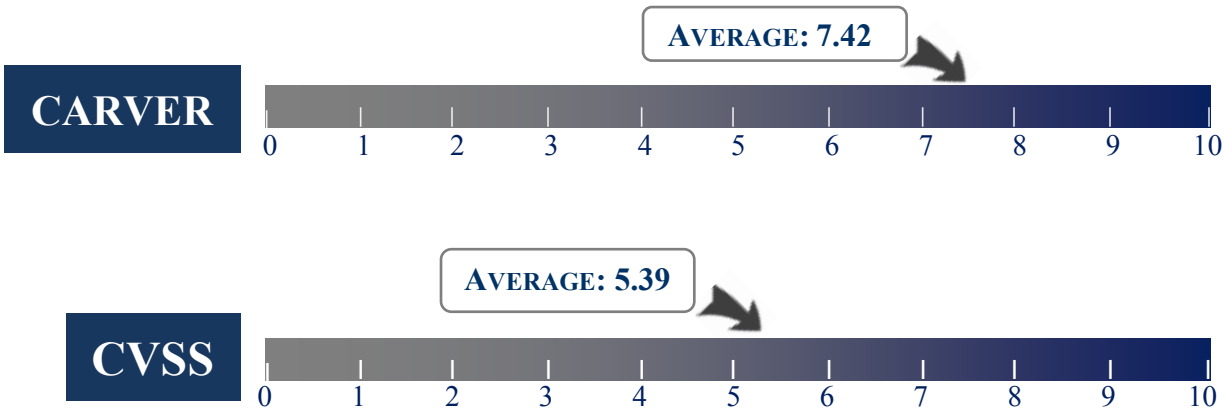
Findings Overview

The combined dataset from Cyber Hygiene and RVA testing in FY14 represents the largest amount of data collected in a single year by NCATS. Cyber Hygiene, which includes Domain Name System Security Extensions (DNSSEC) compliance checks, is an automated recurring scanning and vulnerability service. Each RVA is a highly customized engagement dependent on security professionals to perform detailed, interactive testing and analysis. Notably, Cyber Hygiene and RVA services are offered upon request; therefore, these results do not represent a comprehensive assessment of any particular industry or sector or of cyber security in general.



NCATS Risk-Based Results

NCATS uses two ranking systems to analyze assessment data: CARVER and CVSS. CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognizability), helps identify the overall risk to high priority systems during RVA engagements. The Common Vulnerability Scoring System (CVSS) is an industry standard used to rank vulnerabilities by severity and is used in the Cyber Hygiene service. A lower score corresponds to less risk for an assessed a system (CARVER) or vulnerability (CVSS). The average score is based on all findings and vulnerabilities detected during FY14.



Year-End Engagement Report FY14

Risk and Vulnerability Assessment

The RVA's two main goals are to:

- Help secure individual stakeholders against known vulnerabilities and threats by providing mitigation strategies to reduce risk;
- Aggregate vulnerability data so policy makers can make informed decisions regarding the security and safety of information systems.

A RVA is conducted by expert DHS analysts using open source and commercial security tools to perform vulnerability scanning and manual penetration testing. Each engagement is built to determine whether and by what methods an adversary can defeat security controls on a network. The RVA provides the individual stakeholder with a report that identifies vulnerabilities, provides mitigation steps, and ensures that the overall security implementation provides the protection that stakeholders require and expect.

RVAs incorporate two methods of testing: Automated Scanning and Manual Testing. Automated scanning utilizes computerized tools , which produce results that are interpreted by NCATS analysts to find valid vulnerabilities. Manual testing involves highly trained engineers employing a hands-on method to discover, validate, and exploit vulnerabilities.

NCATS conducted 39 RVAs in FY14, capping a year of strong growth as the program branched out beyond Federal Government and delivered services to SLTT and critical infrastructure stakeholders. Of the 344 findings discovered during the RVAs in FY14, the top findings and method of testing are outlined below:

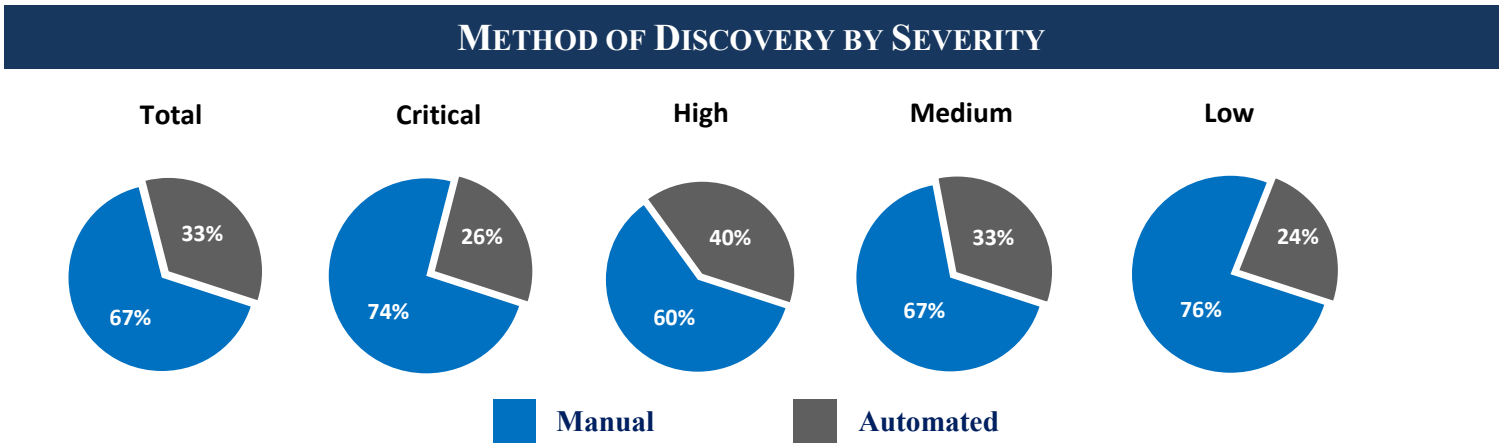
TOP THREE FINDINGS & MAIN METHOD OF IDENTIFICATION

1. Patch Management (88 percent found with automated testing)
2. Sensitive Business Data Disclosure (100 percent found with manual testing)
3. Cross-site Scripting (63 percent found with manual testing)

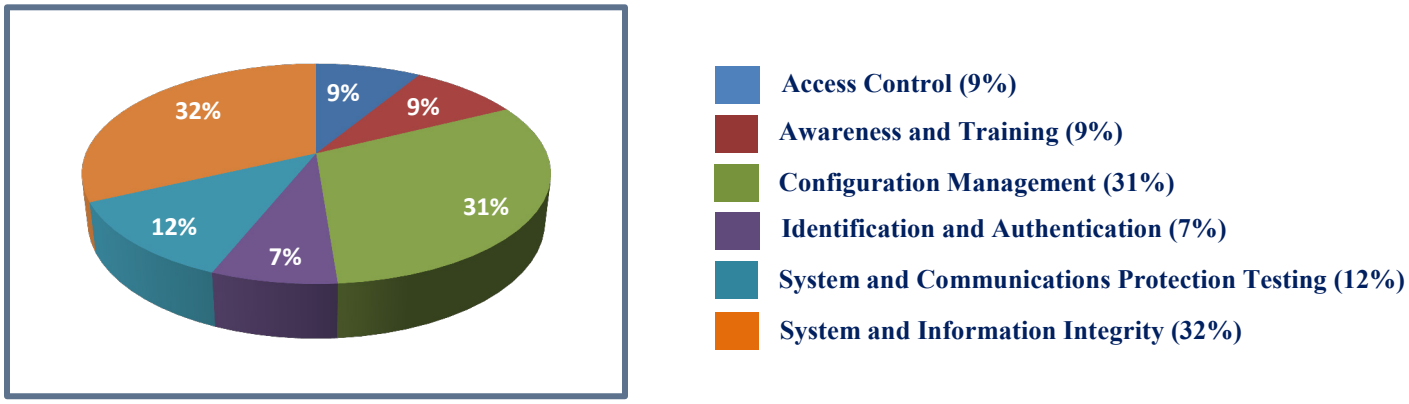
Findings by Severity

	Critical	High	Medium	Low/Info	Total Findings
Total Findings	46	136	104	58	**344**
Percentage	13%	40%	30%	17%	**100%**

Manual Testing was required to identify 67 percent of all findings and 74 percent of all critical findings.



The RVA findings were mapped to applicable controls as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. The chart below illustrates a mapping of findings in FY14 to the top identified families of controls.



Based on this information, closer scrutiny should be placed on the controls defined in the NIST Configuration Management and Access Control families. NCATS will continue to map the RVA findings against the NIST controls to determine changes or trends that may be occur.

NCATS continues to observe inadequate configuration management as a leading contributor of vulnerabilities and potential system compromises. In addition, default credentials, weak passwords, and inadequate input validation are serious concerns that represent common findings during RVAs, although easily corrected once identified. The availability of open source tools that abuse these common vulnerabilities simplify the process for the attacker, making it relatively easy for even those of moderate or little experience to succeed in compromising these problematic systems. For many of the systems tested, timely patch management and prudent configuration management would significantly reduce the risk of system compromise.

Cyber Hygiene

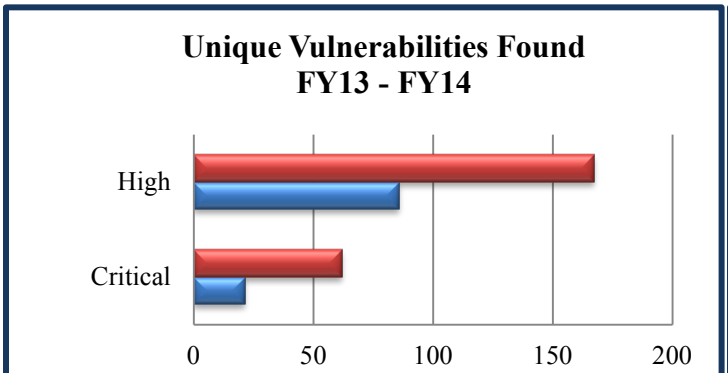
The Cyber Hygiene activities focus on increasing the general health and wellness of the cyber perimeter by broadly assessing Internet accessible systems for known vulnerabilities and configuration errors on a persistent basis. As potential issues are identified, the NCATS team works with impacted stakeholders to proactively mitigate risks to systems prior to exploitation by malicious third parties. Benefits to stakeholders include: third-party review of external networks, no-cost scanning services, reduction of risk, a view of how the assessed network appears to an attacker, and actionable data for quick mitigation/results.

68 Participating stakeholders

384 Cyber Hygiene scans conducted in FY14

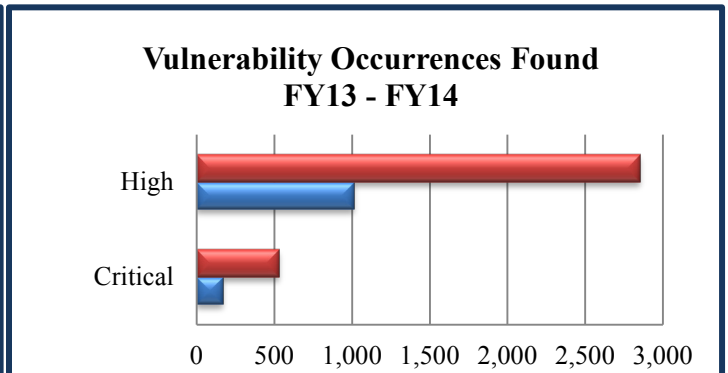
16.9 Million Scanned IP addresses

The NCATS team conducted 384 Cyber Hygiene scans representative of 68 stakeholders and experienced an increasing demand from FY13 to FY14 of 347 percent. During FY14 the NCATS team scanned over 16,900,000 IP addresses. Using the NIST National Vulnerability Database as the benchmark of defined vulnerabilities, Cyber Hygiene assessments identified 531 unique vulnerabilities in FY14. From those unique vulnerabilities the team identified a total of 65,776 vulnerability occurrences.



	Critical	High
FY14 Total	62	167
FY13 Total	21	86

FY14 Medium = 271 and Low = 31
FY13 Medium = 177 and Low = 21



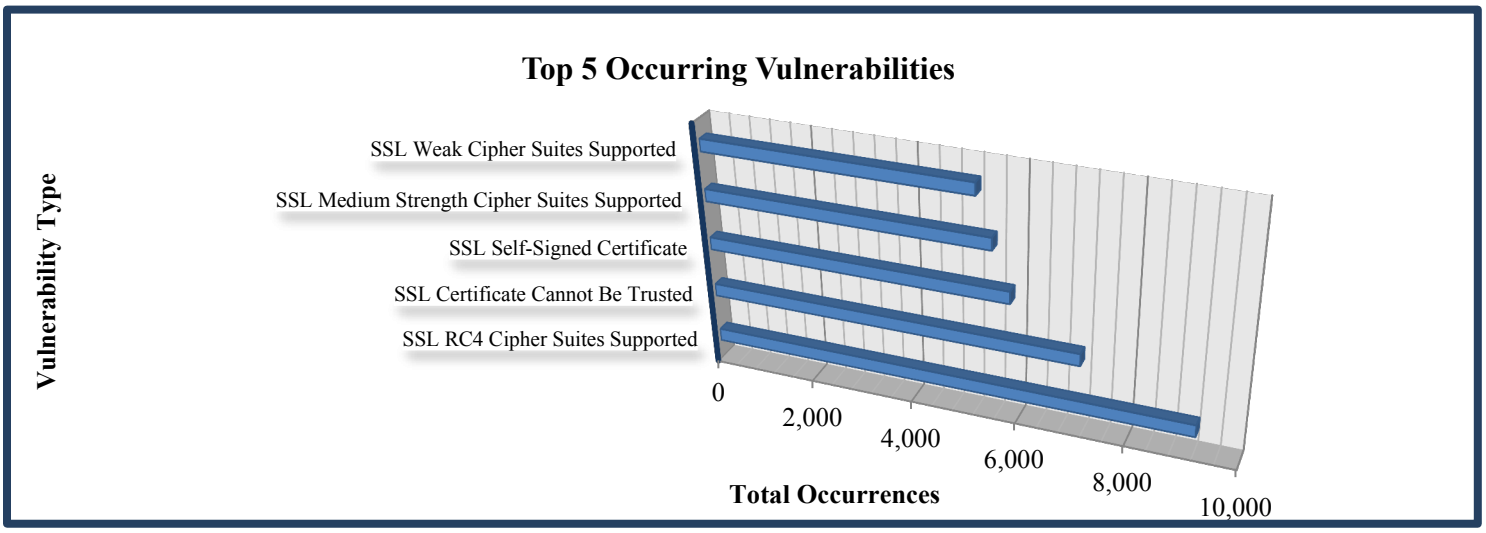
	Critical	High
FY14 Total	530	2,852
FY13 Total	169	1,011

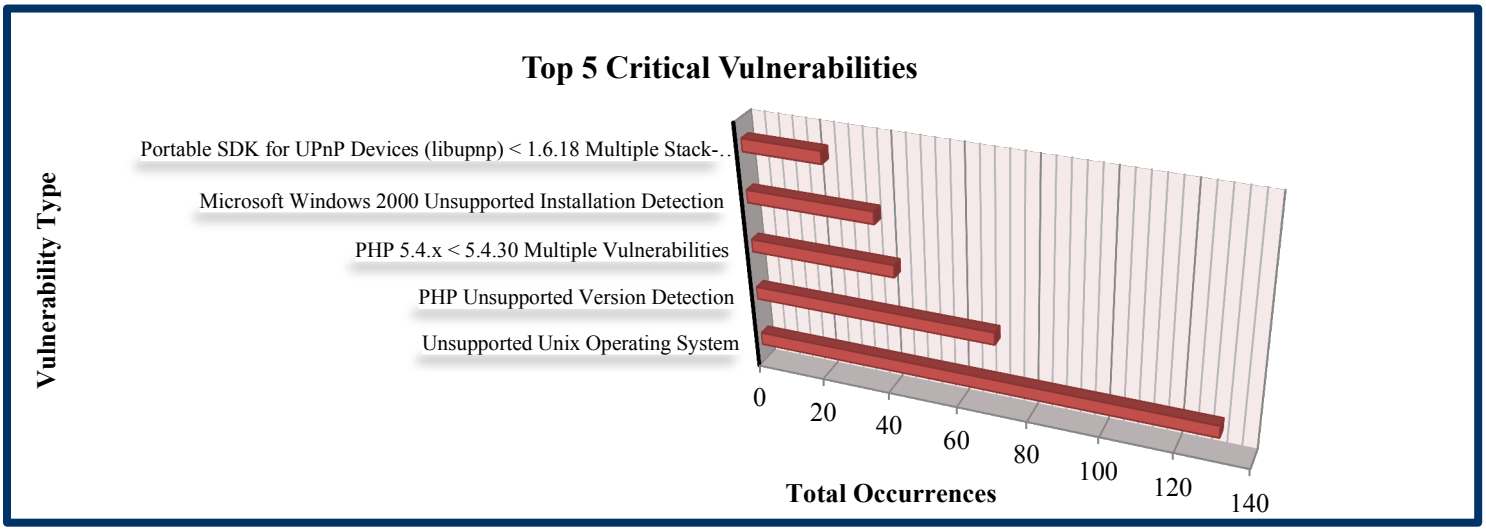
FY14 Medium = 42,816 and Low = 19,578
FY13 Medium = 12,809 and Low = 2,865

The NCATS team utilizes the industry standard CVSS to rank vulnerabilities by severity, with a higher score representing a more significant risk. The average CVSS score for vulnerable hosts was 5.39 on a scale of 0 to 10.

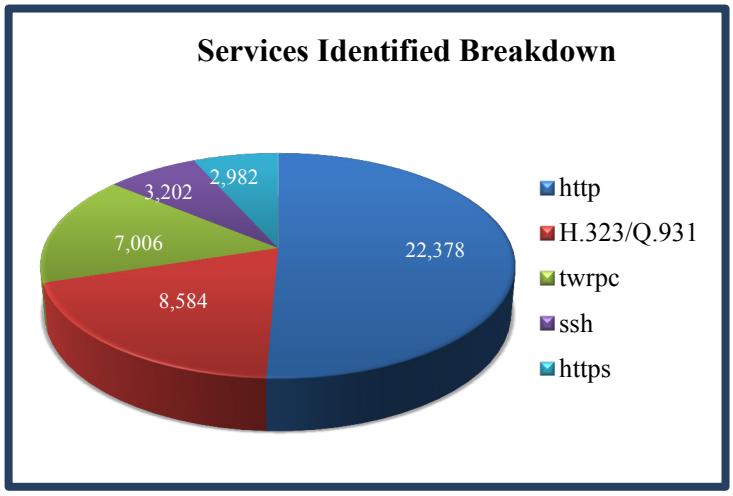
The most common vulnerability in FY14 Cyber Hygiene scans was *SSL RC4 Cipher Suites Supported* with 9,216 occurrences. The top two critical vulnerabilities were *Unsupported Unix Operating System* and *PHP Unsupported Version Detection* with 131 occurrences and 70 occurrences respectively. The NCATS team found stakeholders averaged 4.72 vulnerabilities per vulnerable host.

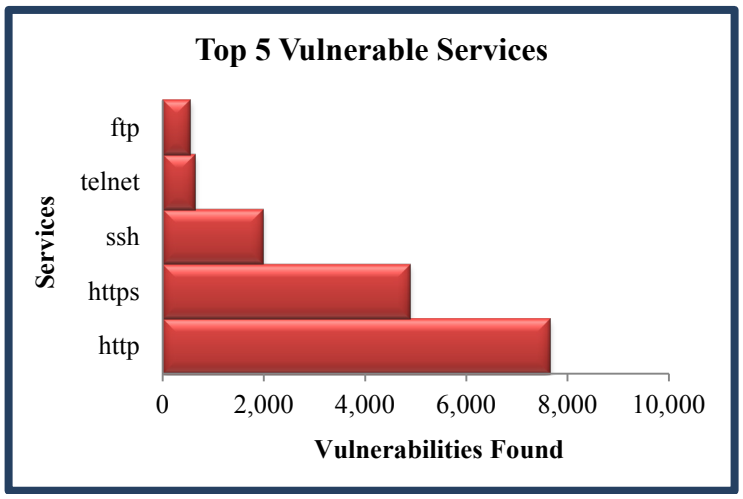
VULNERABILITY FINDINGS



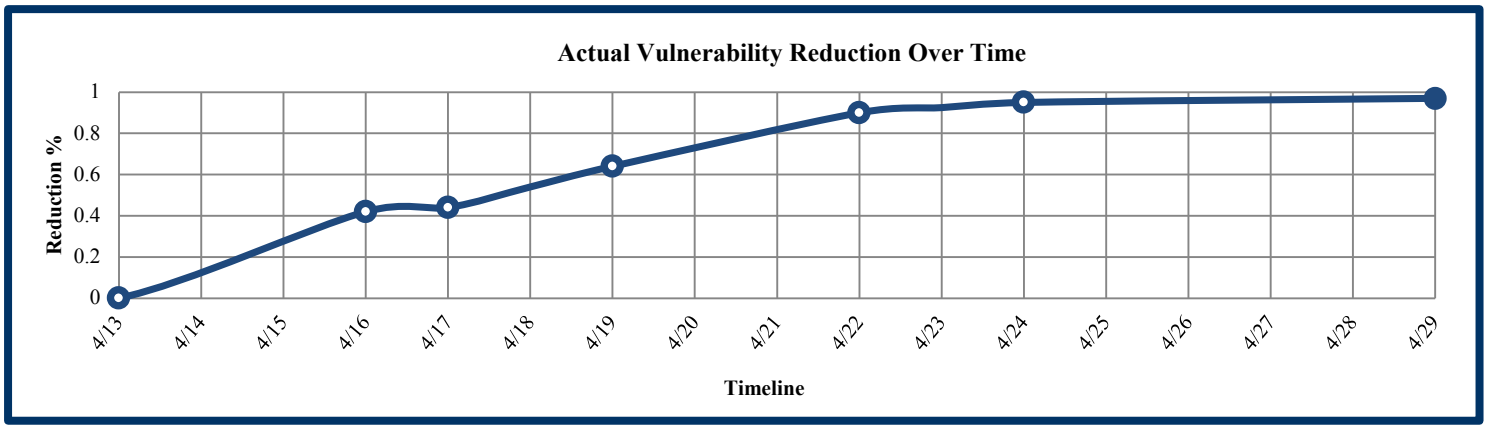


TOP SERVICES & VULNERABLE SERVICES IDENTIFIED





The Cyber Hygiene service found that *http* was the most frequently identified service with over 22,000 instances. The other top four services identified represent a much smaller percentage and are broken down in the figure above. The top five vulnerable services are shown in the figure with *http* registering over 7,600 instances (42%). Of note, 1.7 million ports scanned were identified as *tcpwrapped*. Services being *tcpwrapped* indicates that network services are intentionally secured or being reported as obscured and is a very positive result and good security practice.

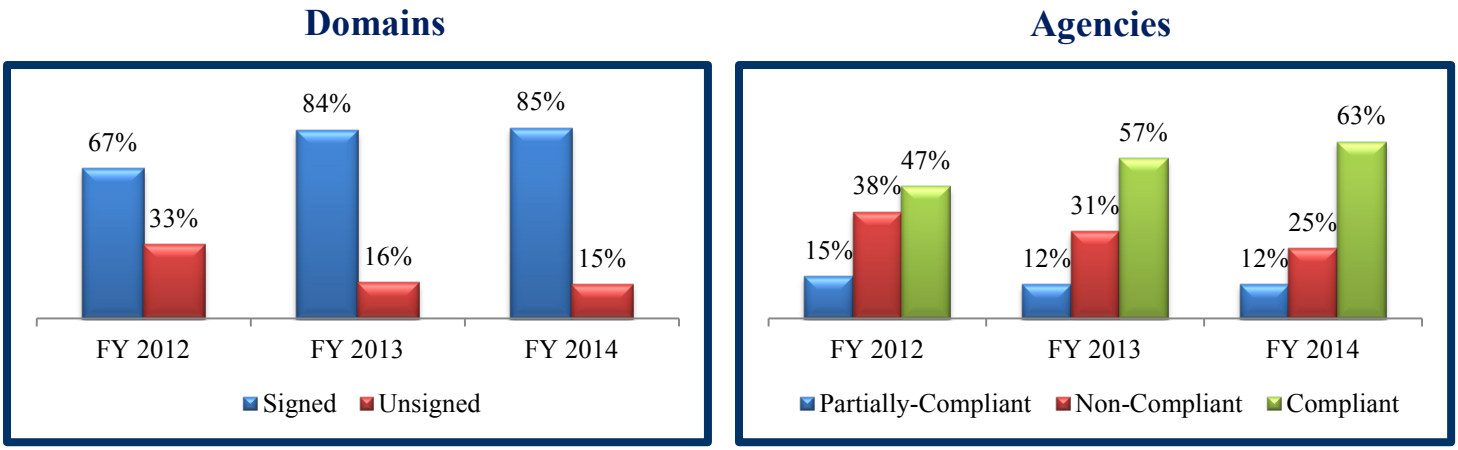


In early April 2014, DHS learned of the Heartbleed vulnerability as it emerged and set out to assess its potential impact on and scope across the Federal Government. The NCATS team worked with more than 100 federal agencies to receive authorization to begin scanning, identify public IP address space, schedule times to conduct scanning, and deliver individualized reports and results to each agency. A 99% reduction rate of Heartbleed instances occurred from first scan to last scan.

With the overall success of Heartbleed activity and the need to reduce exposure times, DHS is now authorized to provide to federal civilian agencies proactive vulnerability scanning under the Office of Management and Budget (OMB) Memorandum (M-15-01), *FY 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices*. This new guideline allows the NCATS team to utilize the Cyber Hygiene service

to scan federal Internet-reachable hosts on a persistent basis. In addition, for cases of a large scale vulnerability release (e.g. Heartbleed) M-15-01 allows DHS to effectively execute scans under emergency circumstances. While M-15-01 is only directed at Federal agencies, other Cyber Hygiene stakeholders from SLTT and critical infrastructure entities will benefit from these same proactive scans upon their request.

FY 2012 - FY 2014 DNSSEC Compliance Trends



The DNSSEC testing is a subset of Cyber Hygiene focusing on domain name server security within the federal government. This effort is in support of the OMB memo M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*, which requires federal agencies that have registered and are operating second level .gov Internet domains to deploy DNSSEC. To assess the overall level of federal progress in meeting this mandate, NCATS conducts weekly DNSSEC scans and the results are distributed to each federal agency.

At the end of FY14 the Federal Government had 1,169 of 1,369 (85 percent) domains fully compliant with DNSSEC. Agencies have made consistent progress toward implementing DNSSEC across all of their domains. The agencies that implemented DNSSEC on 90 percent or more of their domains increased by 10 percent (67 to 74 agencies). *Non-compliant* agencies dropped by 17 percent (36 to 30 agencies) and *Partially Compliant Agencies* remained unchanged with 14 agencies.

Conclusion

The FY14 *NCATS Year-End Engagement Report* provides NCATS stakeholders with a non-attributable report summarizing the baseline findings of the RVA and CH services across the Federal Government, SLTT, and private stakeholders who requested and received services in FY14. Because the NCATS services are not presently being utilized by all government agencies, this report provides only a partial snapshot of the government cybersecurity posture in FY14. However, general trends are evident among the results presented here, such as the lack of configuration/patch management and the prevalence of sensitive data disclosure. Additionally, trends indicate that the Federal Government is improving its overall cybersecurity posture, with a leading example being a three year trend of increasing DNSSEC compliance across individual federal .gov domains and whole agencies. as well as the rapid response the Federal Government showed in response to the Heartbleed vulnerability.

The services offered by NCATS, as outlined in this End-of-Year Report, are a single part of the cybersecurity solution and provide an independent third party review of a stakeholder's operational security. In FY15, NCATS will persistently scan federal agencies with the Cyber Hygiene service and pilot additional services to the Risk and Vulnerability Assessment. NCATS will host various cyber talks and symposiums throughout FY15 to share techniques, lessons learned. and general information security knowledge.

The demand for RVA and CH testing continues to grow. As this trend continues into FY15, the NCATS team anticipates increased participation from CIOs, CISOs, and technical communities throughout the Federal Government; SLTT governments; the private sector; and critical infrastructure stakeholders. Over time, the data derived from these activities will reflect substantial cyber technical trends that will support and enable senior leaders to adequately invest in and execute approaches for more resilient and robust cybersecurity in their organizations and for our nation.

Contributors

This document was developed by individuals in the Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity and Communications, National Cybersecurity and Communications Integration Center.

For their hard work and dedication in managing the program strategy, staffing the assessments, building the tools, and sacrificing nights and weekends to make this nation more secure, NCATS wishes to acknowledge and thank the following group of determined government employees, contractors, and interns who made this report possible.

Mike Albrethson
Don Benack
Steve Borosh
Paul Brandau
John Bush
Carl Deputy
Mark Feldhousen
Jason Frank
Chris Hernandez
Jason Hill
Willio Jean Paul
Rob Karas
Brent Kennedy
Dan Klinedinst
Rick Lichtenfels
David Link
Matt Maley
Sam Manickam
Sean McAfee
David McGuire
EmilyJane McLoughlin
Lorenzo Miller
Alex Norman
Dr. Andy Ozment
Kevin Partridge
Kyle Pellegrino
Dave Redmin
Will Schroeder
Hal Snedden
Roberta Stempfley
Kelly Thiele
Danny Toler
Brig. Gen.(ret) Greg Touhill
TJ Trajano
Chris Truncer
Ken Vrooman
Scott Wallace
Mike Warren
Mike Wright
Jon Yates

Contact

For comments or questions, please contact DHS NCATS at NCATS_Info@hq.dhs.gov.

Appendix A: Glossary

Active Hosts	A subset of Total Hosts that respond to a scan looking for hosts which are responsive on a network.
CH Vulnerability Severity Levels	All Cyber Hygiene vulnerability severity levels are based on CVSS scores from 0 to 10. "Critical" findings have a score of 10, "High" findings are less than 10 but greater than or equal to 7, "Medium" findings are less than 7 but greater than or equal to 4, and "Low" findings are less than 4.
DNSSEC	Domain Name System Security Extensions
FY	Fiscal Year - U.S. Federal Government – October to September
RVA Vulnerability Severity Levels	Critical – Vulnerabilities pose an immediate and severe risk to the environment because of the ease of exploit and/or potential severe impact. High – Intruders may be able to exercise full control on the targeted device. Medium – Intruders may be able to exercise limited control of the targeted device. Low – Vulnerabilities that are an item of interest, but are not normally exploitable or present minimal risk.
Sensitive Data Disclosure	Information an attacker can use to negatively impact business operations or system functionality.
Unique Vulnerabilities	The count of vulnerabilities detected on an agency's network that does not include duplicate instances of a single vulnerability. If a single vulnerability is detected on multiple hosts, the vulnerability is only counted once towards the Unique Vulnerability total.
Vulnerability Occurrences	The number of all vulnerabilities totaled across agency's hosts. How many vulnerability occurrences an agency has overall may include multiple instances of a unique vulnerability because multiple hosts can have the same vulnerability.
Vulnerable Hosts	A subset of Active Hosts that have at least one detected vulnerability.