protiviti®

Face the Future with Confidence

2018 Security Threat Report

Assessing Nine Years of Cyber Security Vulnerabilities and Exploits

Internal Audit, Risk, Business & Technology Consulting

Executive Summary

Finding the right words to describe the magnitude of cyber security today is like trying to define the size and splendor of the Grand Canyon to someone unfamiliar with the natural wonder of the world. News of massive data breaches continues to make headlines. Among the largest breaches to date, one of the major consumer credit reporting agencies announced last year that hackers accessed its store of Social Security numbers, driver's license data, birth dates and other personal information on more than 140 million consumers. A decade ago, such news would have been unimaginable. But sadly, over the last several months, disclosures of significant cyber security breaches have become routine as organizations increasingly rely on vulnerable digital technologies and third-party service providers.

At the same time, cyber criminals are becoming more creative and sophisticated. New cyber threats emerge daily that put any number of business systems at risk, and companies face a monumental challenge to keep pace with the threats and safeguard their data, particularly their "crown jewels." It's no surprise that cyber security is the chief concern not only for CIOs and IT departments, but also for executive-level management and boards of directors.

This report aims to help organizations address and understand the cyber security landscape by exploring and detailing the most common digital threats today. Since 2009, Protiviti security labs in the United States have performed more than 500 in-depth security scans on behalf of a broad range of organizations to test and assess their IT systems and infrastructure for cyber security risks. Keeping the organizations anonymous, we have compiled and quantified the vulnerability and threat discoveries in our data, offering insights and trends regarding the types of threats organizations are most likely to face, the most frequently perpetrated cyber crimes, the recent acceleration of attacks, and trends in cyber attacks by industry and size, among other views.

In addition, we provide insight into the root causes underlying the vulnerabilities and practical guidance on how companies can protect their information.

In these times of digital treachery, we hope you find this report useful.

Key calls to action we define include:

01 Strong permission and user access controls

02 Employee security awareness

03 Patch management

04 System configuration management

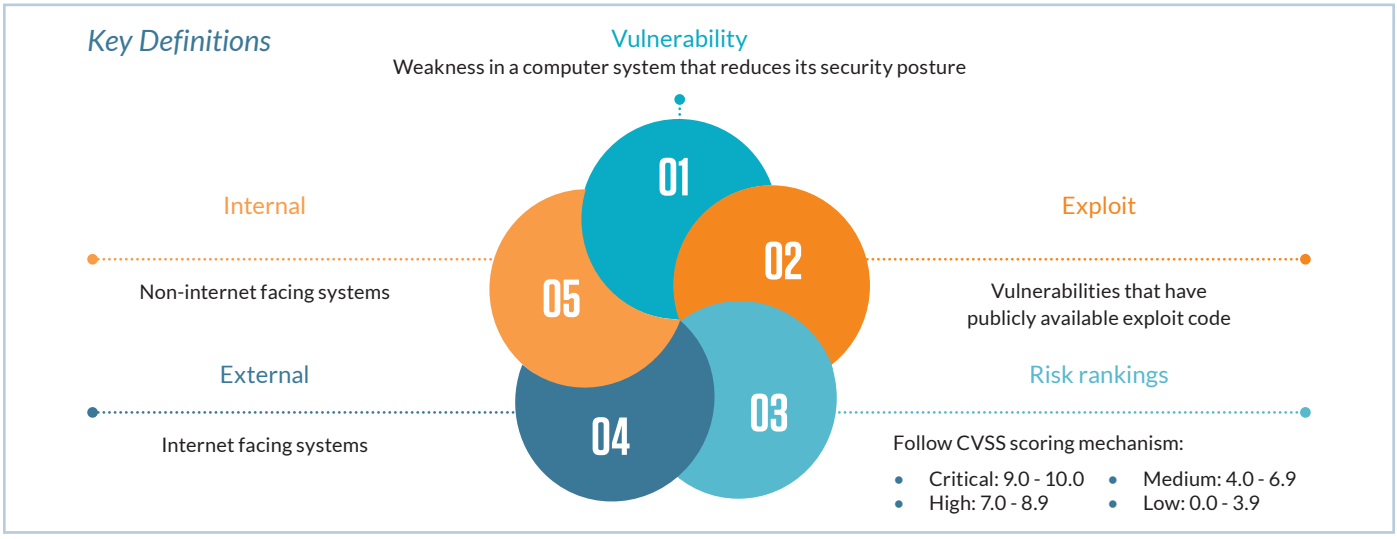
05 Periodic penetration testing

About Our Study

We compiled the data, analyses and trends presented in this report by reviewing information from security vulnerability scans of IT systems of more than 500 organizations in a broad range of industries. Over a nine-year period, Protiviti's security experts were engaged by these companies to scan their networks, detect vulnerabilities, and help fix issues and establish proper mechanisms for monitoring and prevention. This data has been aggregated and analyzed into data points that we believe are both informative and useful for those trying to safeguard their systems.

Some important notes and definitions about the data in our report:

- The scanned data from these engagements was not validated – rather, it is the raw data from a leading vulnerability scanner that the Protiviti teams used.
- The test data is from a broad range of industry organizations:
  - Financial Services
  - Healthcare and Life Sciences
  - Consumer Products and Services
  - Technology, Media and Telecommunications
  - Manufacturing
  - Education
  - Energy and Utilities
- The data contains results from those of internet-facing systems (**external**) as well as systems on the inside of the organization's firewall (**internal**).
- Vulnerability data contained within this study relate to network-related issues only. Web application vulnerabilities are not included. In addition, vulnerability data related to the same missing patch or outdated system versions have been removed, with only the highest total remaining, to reduce repeat items.
- **Vulnerability** refers to a weakness in a computer system that reduces its security posture.
- **Exploit** refers to vulnerabilities that have publicly available exploit code as of the time of testing.
- **Risk rankings** generally follow the standard CVSS scoring mechanism:
  - Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0–3.9.
  - Vulnerabilities are labeled "Medium" severity if they have a CVSS base score of 4.0–6.9.
  - Vulnerabilities are labeled "High" severity if they have a CVSS base score of 7.0–8.9.
  - Vulnerabilities are labeled "Critical" severity if they have a CVSS base score of 9.0–10.0.

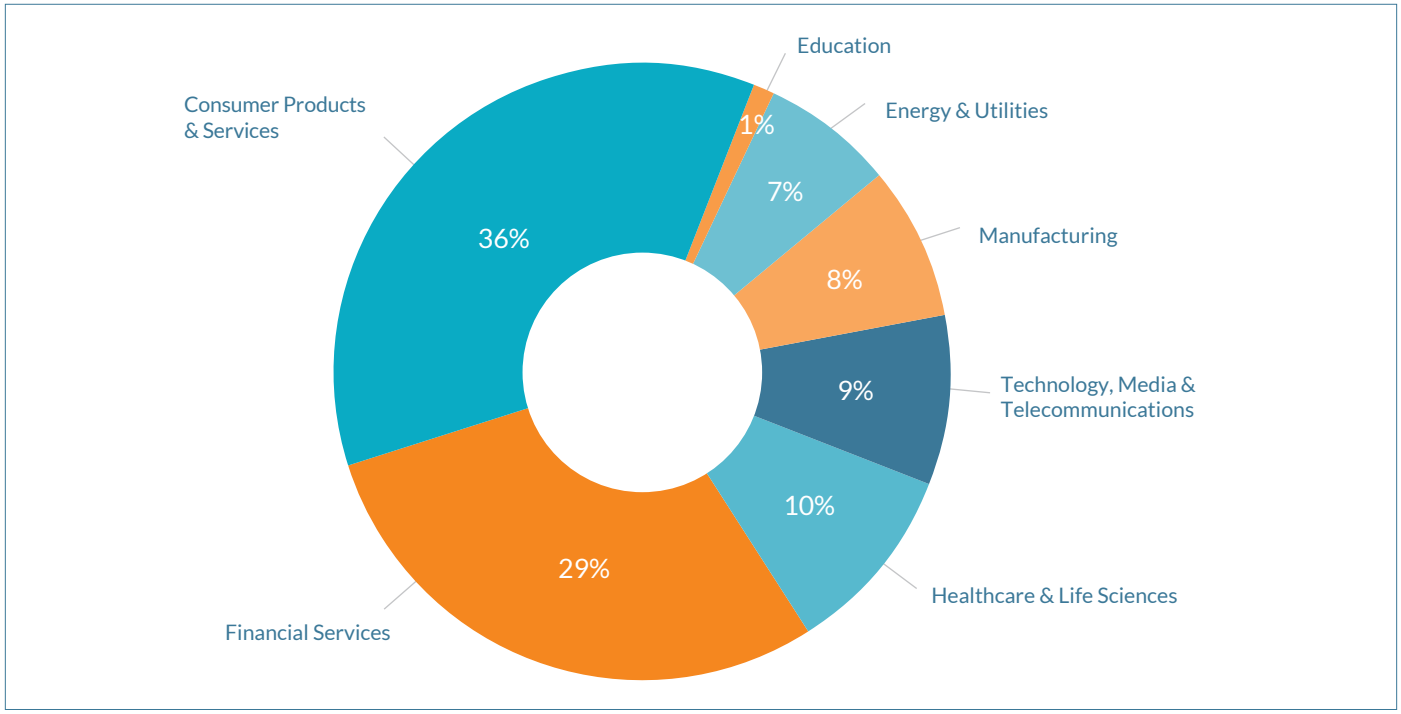


Key Takeaways/Trends and Analysis

Based on the wealth of data taken from nine years' worth of security scans and the trends they reveal, there are a number of key takeaways and learnings:

- Patching, both external and internal, remains a critical issue. In particular, application patching appears to be a more problematic issue than operating system patching.
- Organizations are still running a significant number of unsupported systems.
- There have been consistent challenges with SSL, especially with regard to weak ciphers and diversions. Though the raw number of issues hasn't reached a high level, this is an area for organizations to monitor.
- Not surprisingly, the number of exploits and vulnerabilities organizations have experienced has risen over time. Also of no surprise, the ports with the most vulnerabilities are Windows 445 and web 443.
- Every few years, a major critical exploit comes along that has a drastic impact on the security landscape. Just a few examples include MS08-067, Heartbleed, Shellshock (CVE-2014-6271), MS17-010 and MS15-034.
- Just under half of the vulnerabilities identified during testing have a publicly available exploit.

Organizations Included by Industry and Number of Scans/Tests Performed



Call to Action

Regardless of an organization's industry or size, developing, establishing and implementing five basic security principles will dramatically reduce an organization's risk of a security breach. Organizational networks are only as strong as their weakest link. As such, each of these areas needs to be looked at, evaluated and improved individually and collectively in order to raise the bar high enough so that a non-targeted attacker will be compelled to move on to the next network.

The five items are:

1. **Strong permission and user access controls** – Maintaining strong access controls is one of the primary ways to protect against a breach. Seemingly simple steps such as ensuring appropriate permissions, reducing the number of powerful administrative accounts and changing default passwords significantly reduce the attack surface for a hacker. Software, systems and devices are often preloaded with default permissions, usernames and passwords that are easily identifiable through a quick internet search or system query. Attempting to access systems with default permissions and guessing these usernames and passwords often is one of the first steps an attacker will take when attempting to gain control of a system.

   Organizations that periodically check their network for default permissions/credentials and implement this change as part of the standard system deployment procedures reduce the likelihood of one or more attackers gaining easy access to a network.

2. **Employee security awareness** – Without strong employee security awareness, attackers can manipulate and prey on human emotion and behavior to greatly reduce the effectiveness of technology, often very expensive, that the organization put in place to protect its networks. Social engineering attacks try to obtain information that should not be disclosed and could facilitate gaining unauthorized access to companies' private data and resources. Examples of this include seeking information required to reset and recover an employee's password or any other important information through electronic (phishing) or physical means, or through phone calls.

   Strong security awareness programs provide and reinforce security awareness communications and training provided to employees. Communications inform employees and other users of the latest security threats, activities the organization is taking to mitigate these risks, and measures that users can take to protect themselves and contribute to promoting a secure office environment. Periodic communications also stress proper password protection and management, as well as provide employees with appropriate steps to take when they feel that social engineering techniques are being attempted.

3. **Patch management** – As noted in the threat data presented in our report, most vulnerabilities can be remediated and/or are the result of a system not being properly patched. This not only applies to operating systems, but also to applications. While getting a handle on application patching is often more difficult than on operating systems (largely due to the number of applications and required patches in an environment), it is equally important to protect the organization. Organizations should use automated tools to both identify and apply patches in an environment.

Strong patch management programs have a good handle on the security patch levels on all systems throughout the environment (network devices, operating systems and applications). Systems that are not currently integrated with the existing patch management process are integrated into the centrally managed process. In instances where systems cannot be upgraded or patched due to business constraints, compensating controls (e.g., VLANs or firewalls) should be implemented to protect the rest of the network.

4. **System configuration management** – Strong configuration management ensures that systems are consistently and securely configured across the environment (with exceptions where necessary) to prevent attackers from easily gaining access to systems and data. Areas such as password and audit policies, services, and file permissions are controlled through the configuration management process.

   Organizations with effective configuration management define a standard (usually based on single or hybrid industry standards), deploy it across applicable systems in the environment, and periodically confirm the configurations do not change. This is often controlled centrally to reduce required staff hours as well as lessen the difficulty in determining adherence to defined standards.

5. **Periodic penetration testing** – To ensure the first four calls to action, as described above, are being executed, organizations should perform periodic penetration testing across various pieces of IT infrastructure, including application and network layers. Organizations should commit to performing periodic penetration testing at least annually, though more frequently is better. This periodic testing identifies low-hanging fruit, in terms of security vulnerabilities to address, and keeps the organization up-to-date with the latest tricks and techniques attackers are using. Without periodic testing, organizations may be susceptible to issues outside the scope of the four action items above or may believe certain truths but cannot verify their validity.

Recent breaches continue to reinforce the prevailing wisdom that companies today fall into two groups — those that have been breached and know it, and those that have been breached but don't know it. In addition to preventative measures, organizations must work on maturing detective controls and response procedures. Activities that simulate common attack patterns should be carried out within organizations to determine whether their defenses can detect and respond effectively.

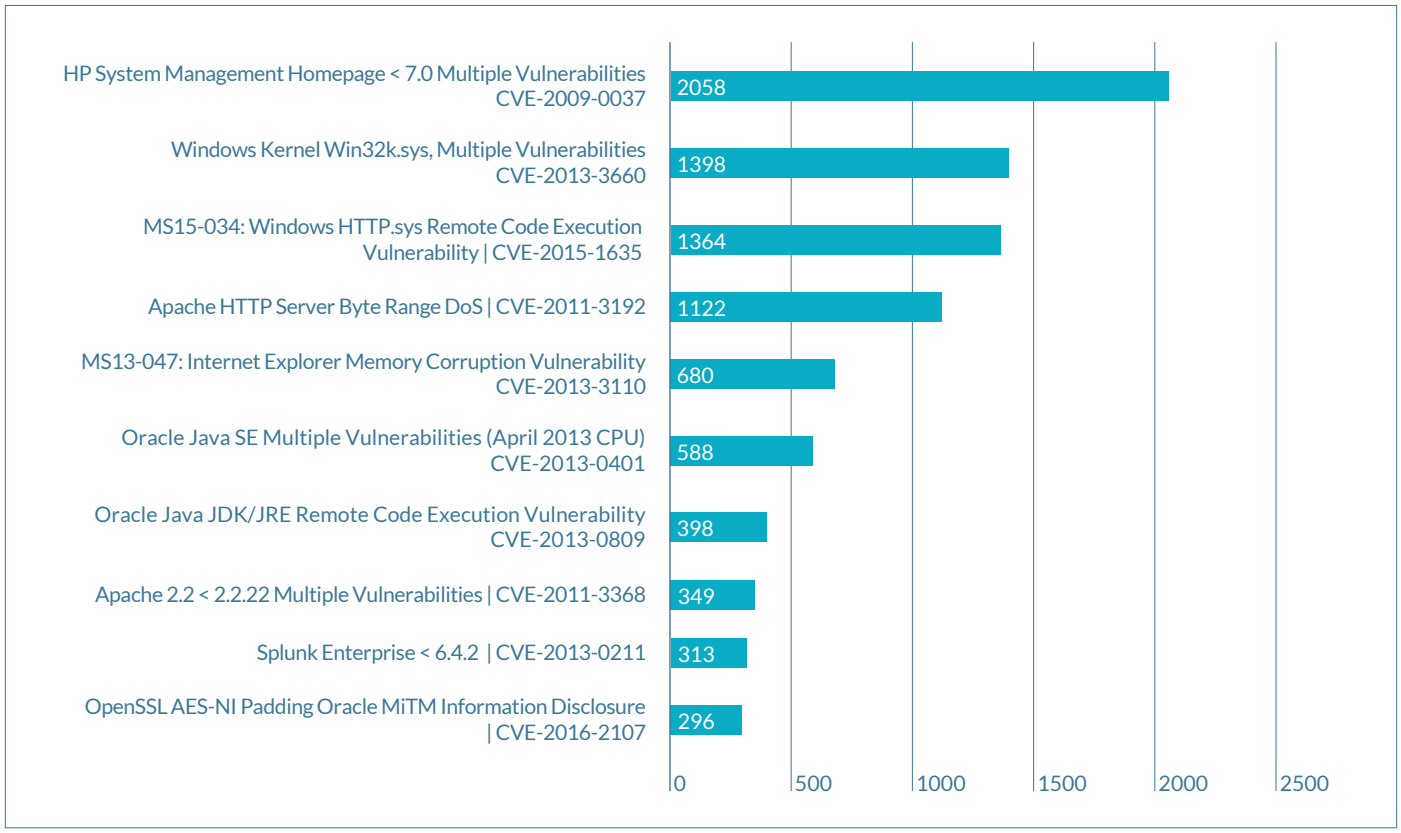
— Andrew Retrum, Protiviti Managing Director – Technology Consulting, Security and Privacy

High-Level Findings (2009 – 2017)

Following are notable high-level findings from Protiviti's vulnerability assessment data. More detailed results are presented starting on page 14.

The graph below identifies the top 10 most common vulnerabilities with a publicly available exploit that existed across all clients and industries.

• • • *Top 10 Most Common* **Exploitable** *Vulnerabilities by Total Count*

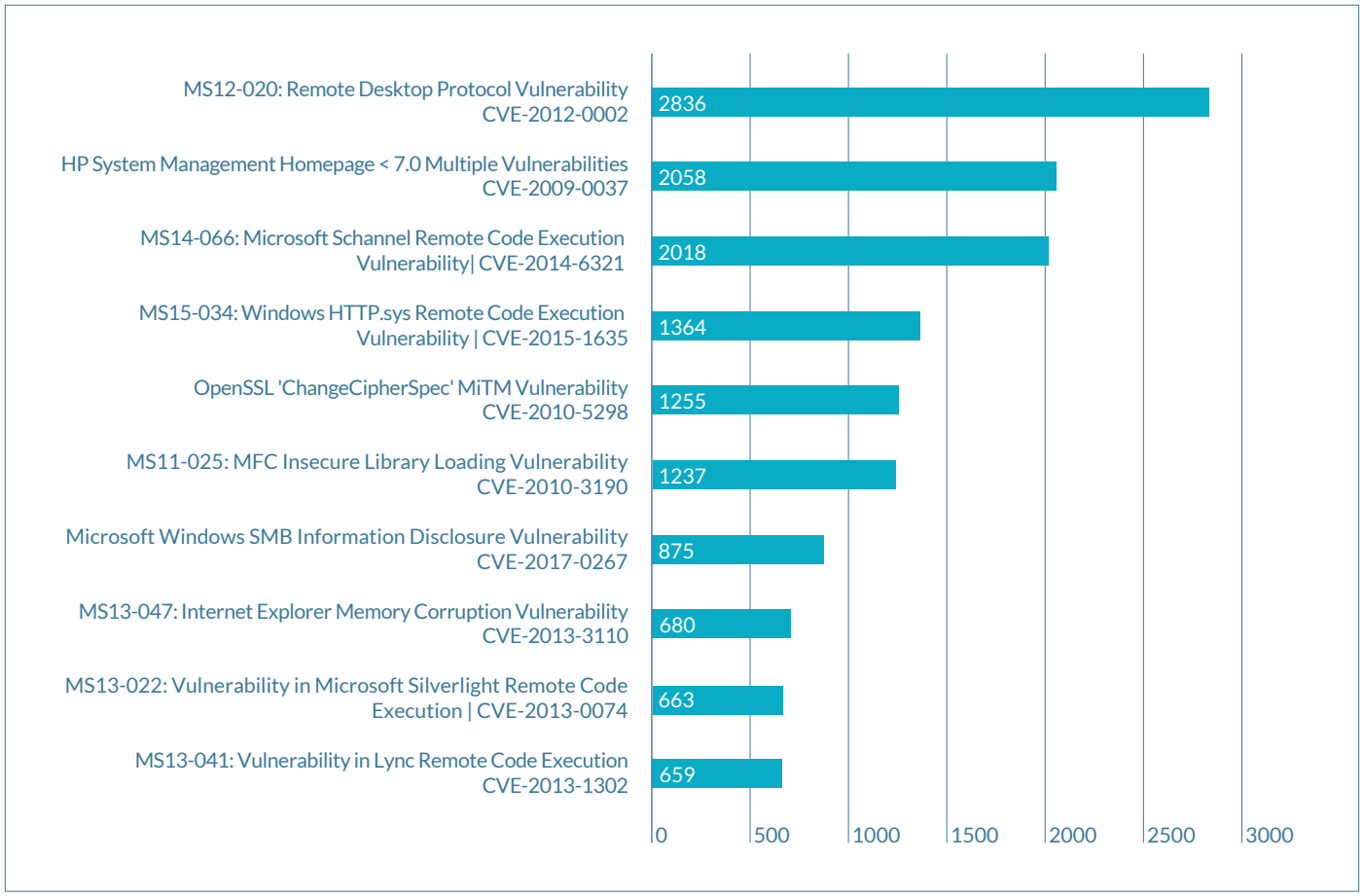


In a recent global survey from Protiviti and North Carolina State University's ERM Initiative, more than 700 directors and C-level executives ranked cyber risk as a top three risk overall, and a "significant impact" risk for businesses in financial services; technology, media and telecommunications; healthcare and life sciences; and energy and utilities. Both directors and CEOs rated cyber as the second-highest risk.

— Source: *Executive Perspectives on Top Risks for 2018*, North Carolina State University's ERM Initiative and Protiviti, www.protiviti.com/toprisks.

The graph below identifies the top 10 most common vulnerabilities, with or without a publicly available exploit, across all organizations and industries.

• • • *Top 10 Most Common High-Risk Vulnerabilities by Total Count*

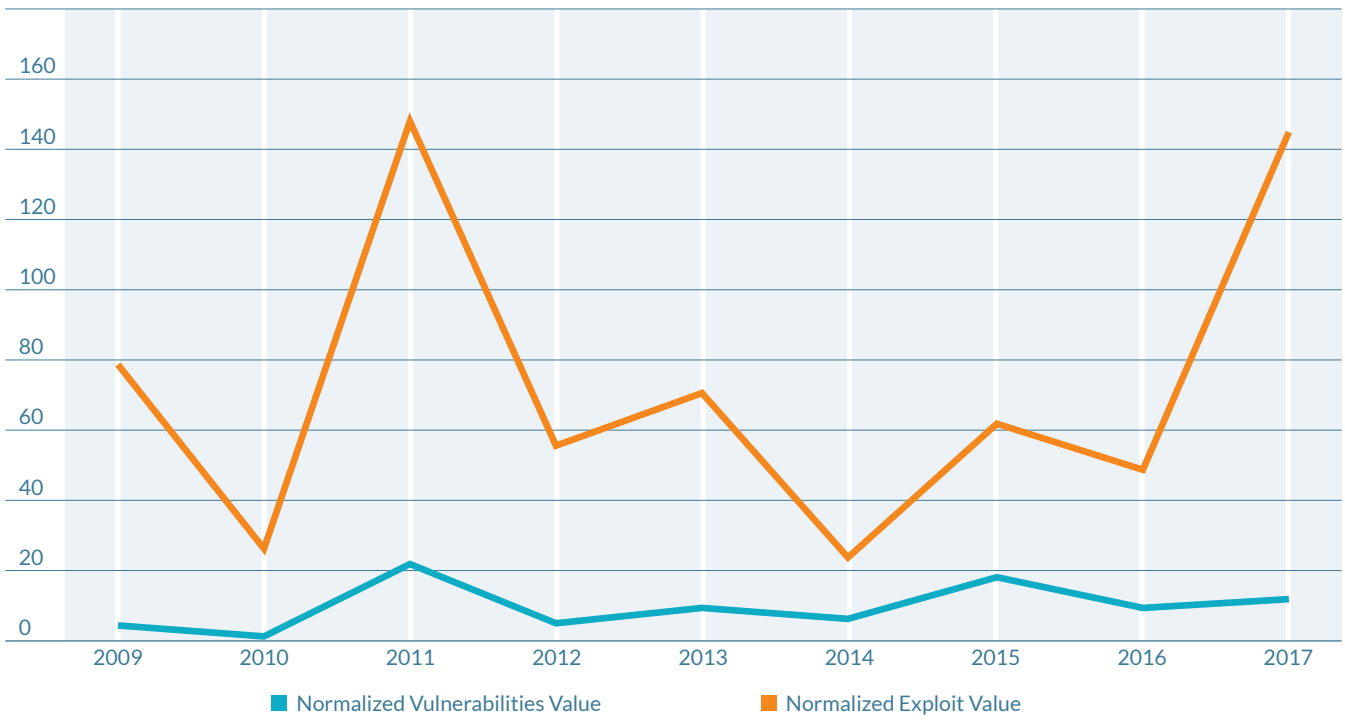


In this modern era of constant attacks, it's expected that public-facing services will be attacked day in and day out. As such, organizations with a well-designed and thoughtful vulnerability management program will do several things, including scanning public-facing systems immediately upon notification of critical vulnerabilities, quickly patching known vulnerabilities for critical public-facing services, and tracking and verifying patch deployment as part of a comprehensive governance process.

— Randy Armknecht, Protiviti Managing Director – Technology Consulting, Cybersecurity

The graph below shows the normalized relationship between vulnerabilities and publicly available exploits over time.

• • • *Number of Unique Vulnerabilities and Exploits Over Time*



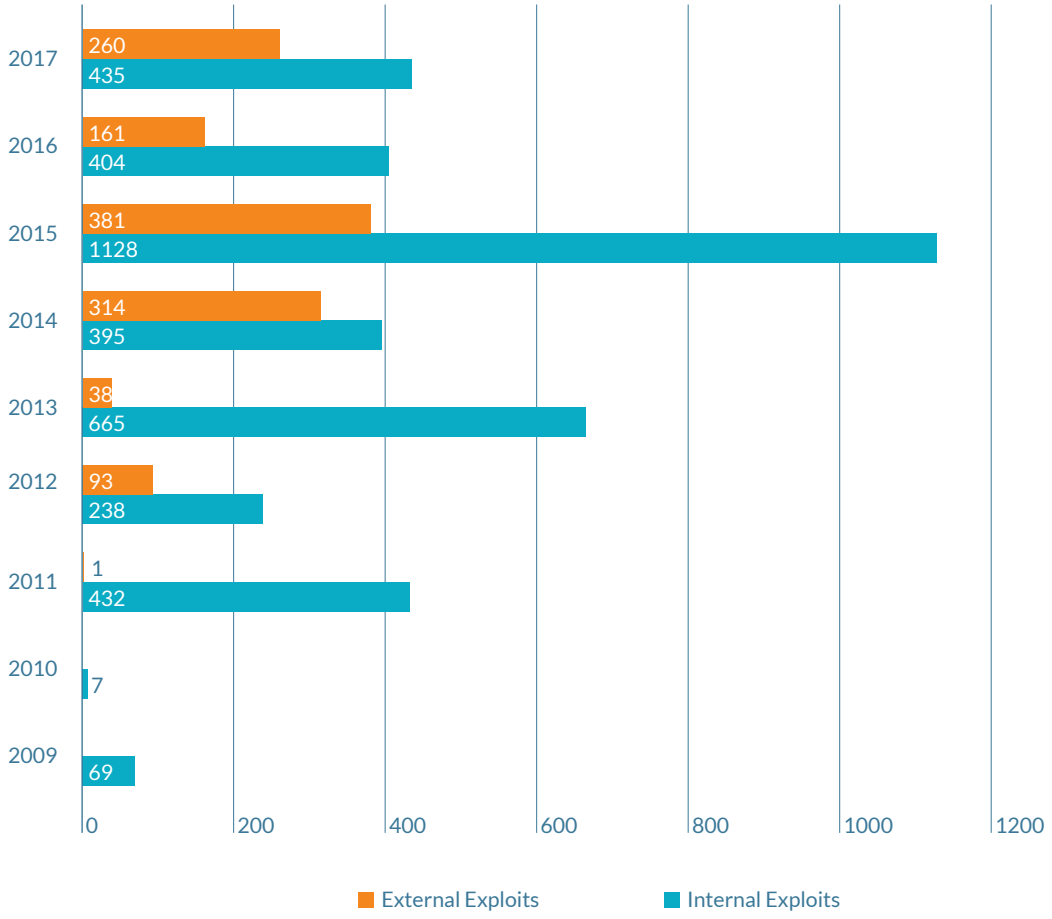
The percentage of increases and decreases in exploits generally correlates with the number of identified vulnerabilities.

Digital transformation and innovative disruption are driving cyber attackers to become increasingly creative. In response, security teams should begin rethinking some of the traditional ways in which they respond to higher threat levels. For example, security groups should consider artificial intelligence and machine learning and how these areas can be applied to cyber security measures. Organizations also should consider the security risks that AI and machine learning pose as these innovations are introduced in other parts of the organization.

— Jonathan Wyatt, Protiviti Managing Director – Leader, Protiviti Digital

The graph below depicts the relationship of uniquely identified publicly available exploits between external and internal infrastructure.

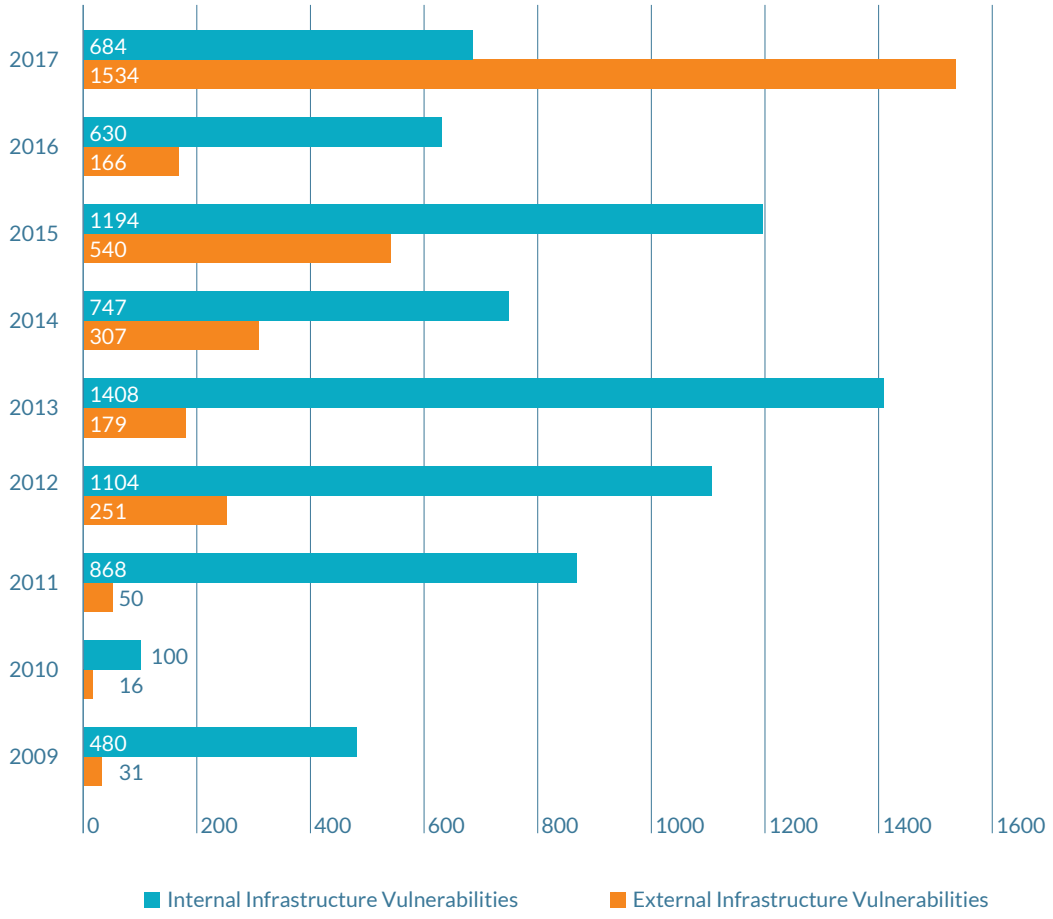
• • • *Number of Unique External vs. Internal Infrastructure Exploits by Year*



As expected, internal networks contain many more exploitable vulnerabilities compared to external networks.

The graph below shows the relationship of uniquely identified vulnerabilities, regardless of whether an exploit exists, between external and internal infrastructure.

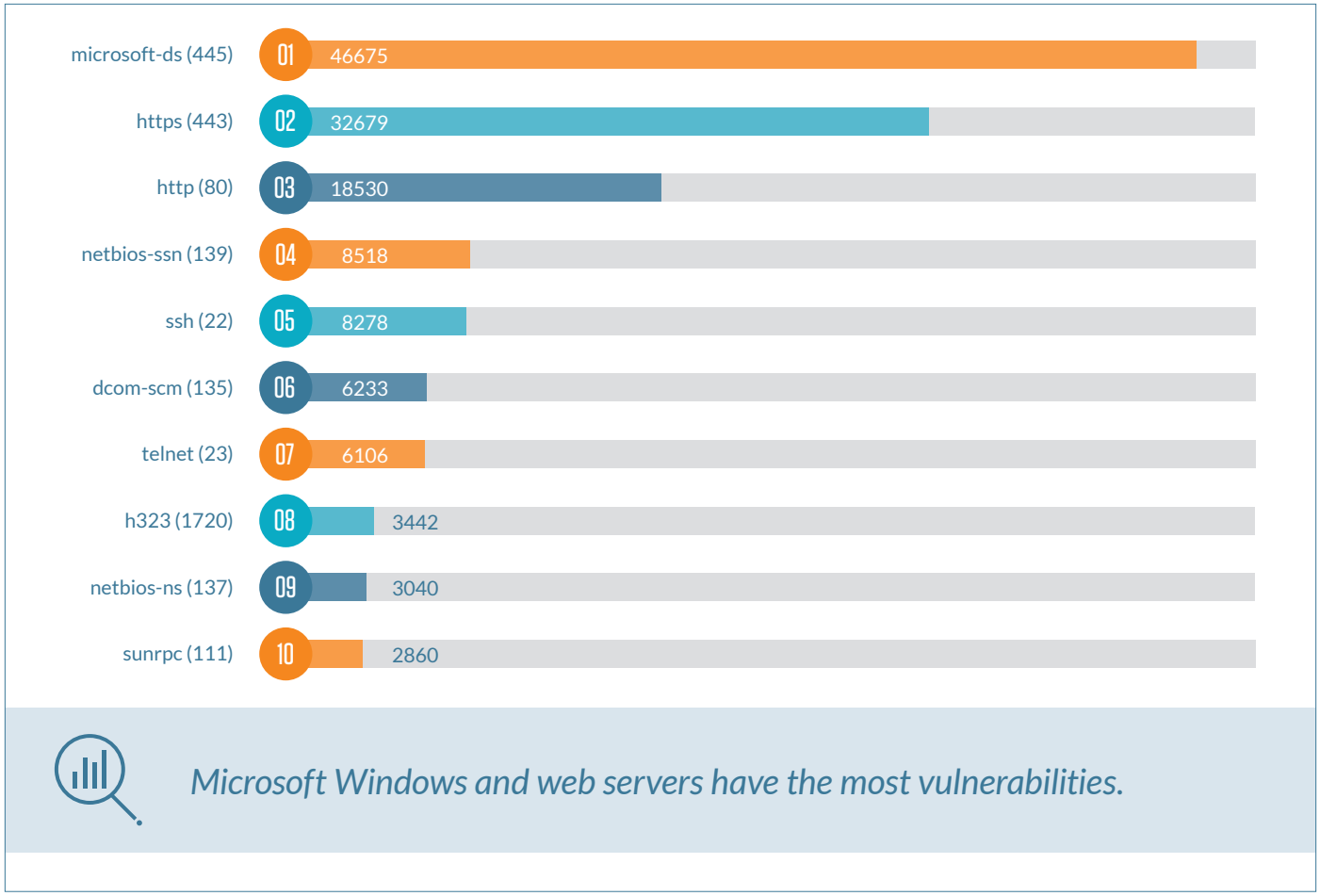
• • • *Number of Unique Vulnerabilities – External vs. Internal Infrastructure*



Unlike previous years, 2017 external vulnerabilities far exceeded internal vulnerabilities due to the increase in items related to SSL and SMB, as well as the number of external tests executed.

Below is a graphic showing the most vulnerable ports from both an external and internal perspective.

• • • *Top 10 Ports with Vulnerabilities — by Total Count*



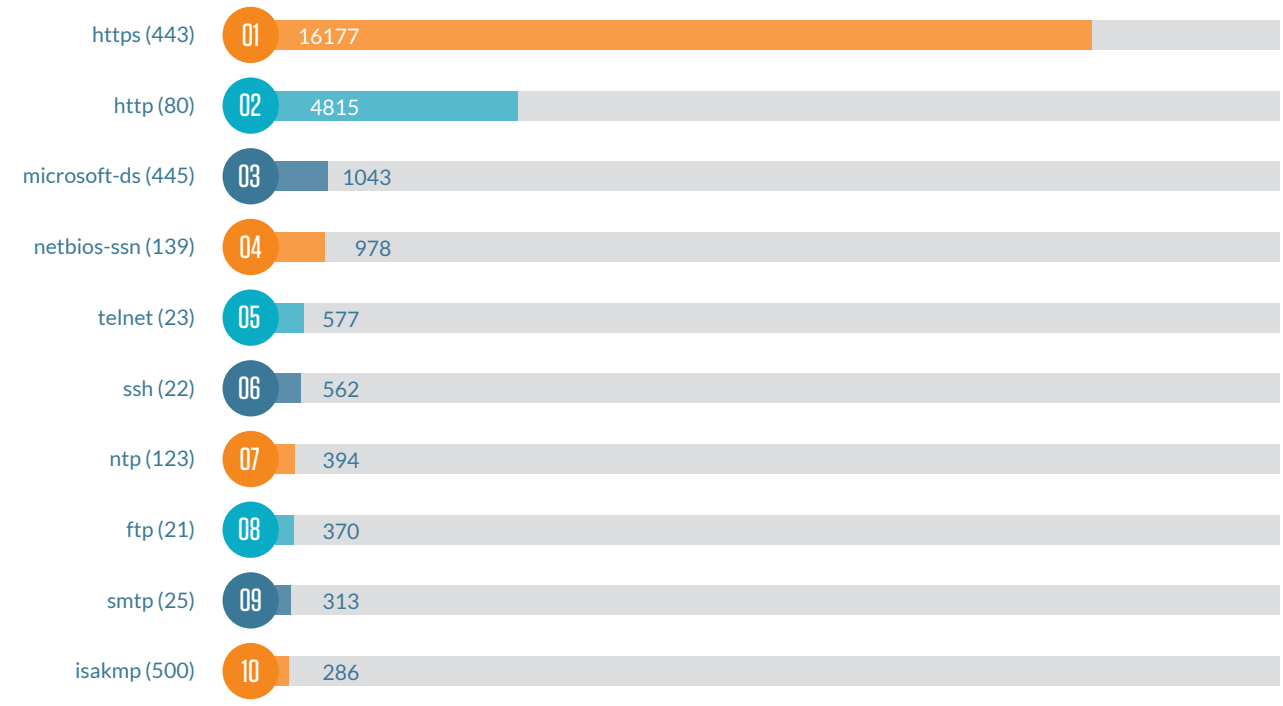
Microsoft Windows and web servers have the most vulnerabilities.

Most technology leaders lack high confidence in their organization's ability to prevent, monitor, detect or escalate security breaches by a well-funded external attacker or by a company insider. However, there is a benefit to not being overconfident: It can stave off complacency while helping to sustain a commitment to continually adapt and improve current practices as cyber attacks grow more sophisticated.

— Scott Laliberte, Protiviti Managing Director – Global Leader, Security and Privacy Practice

The chart below depicts the top 10 most vulnerable ports from an external perspective.

• • • *Top 10 Ports with External Vulnerabilities — by Total Count*



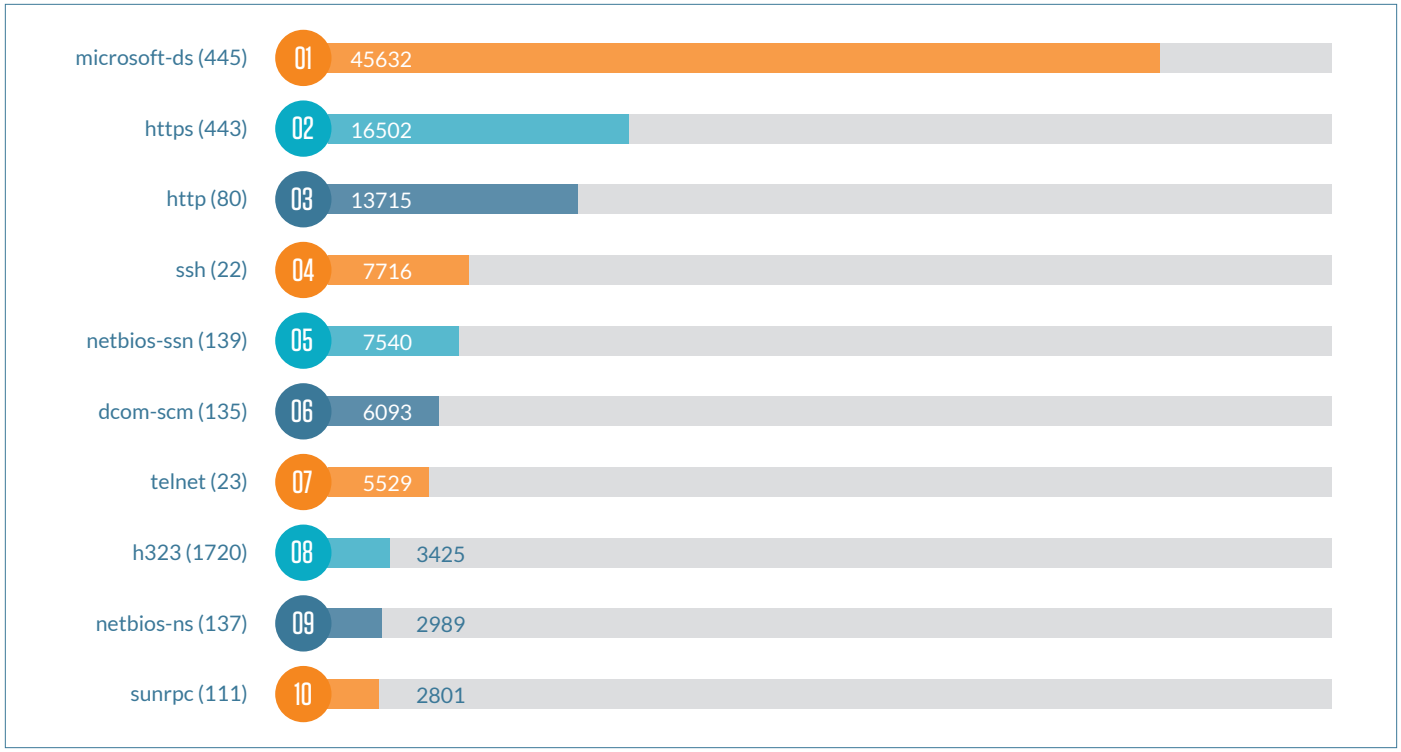
A significant number of companies are leaving Windows systems directly exposed on the internet.

Incident response should be a mainstay of an effective security program. Our research indicates that two out of three organizations have a formal, documented crisis response plan in place. Considering the prevalence of cyber attacks and the growing likelihood of a breach, every organization should have such a plan. It also is important for boards, senior management teams and technology functions to understand that the effectiveness of incident response plans hinges on their execution, and the only way to gauge how these plans will work in reality is to periodically test them in simulations. The most effective incident response plans are "living documents" that are regularly updated to reflect rapidly changing market conditions, emerging security risks and internal changes.

— Michael Walter, Protiviti Managing Director – Leader, Cybersecurity Intelligence Response Center

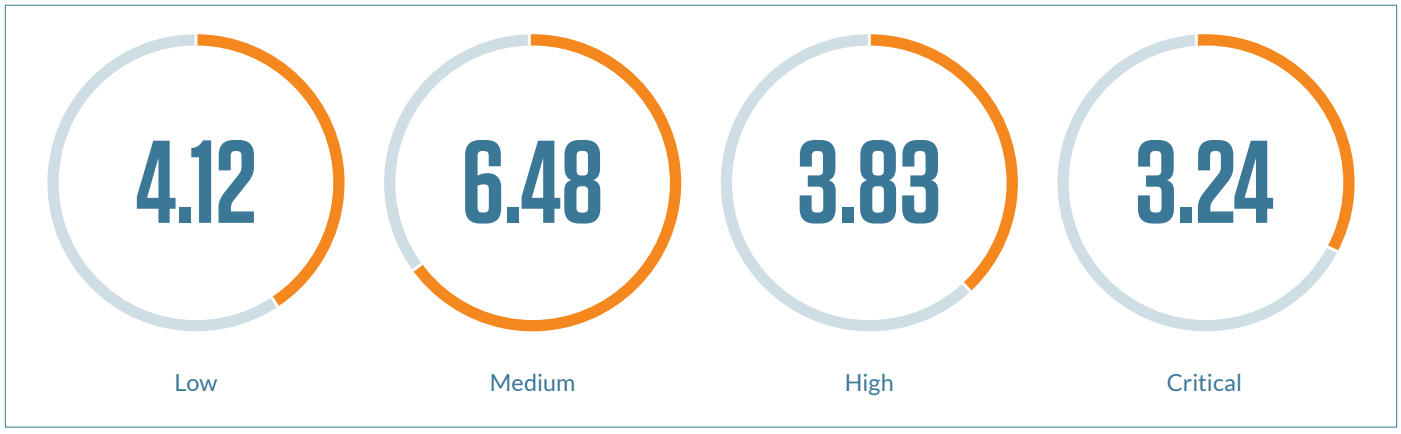
Similar to the chart on the prior page, the graphic below shows the top 10 most vulnerable ports from an internal perspective.

Top 10 Ports with Internal Vulnerabilities — by Total Count



The chart below shows the average age of vulnerabilities by CVSS classification across all industries and systems from 2017 to vulnerability release date.

Average Age of Vulnerabilities (Years) by Severity[1]



[1] Severity rankings are based on the standard CVSS scoring mechanism detailed on page 2.

Detailed Findings (2009 – 2017)

As noted earlier, the prior section provides a high-level summary of key findings from Protiviti's vulnerability assessment data. The following pages contain deeper, more detailed results from this data.

- • • *Top 30 Overall* **Exploits** *by Count*

	Exploit	CVE ID	Count
1	HP System Management Homepage < 7.0 Multiple Vulnerabilities	CVE-2009-0037	2058
2	Windows Kernel Win32k.sys, Multiple Vulnerabilities	CVE-2013-3660	1398
3	MS15-034: Windows HTTP.sys Remote Code Execution Vulnerability	CVE-2015-1635	1364
4	Apache HTTP Server Byte Range DoS	CVE-2011-3192	1122
5	MS13-047: Internet Explorer Memory Corruption Vulnerability	CVE-2013-3110	680
6	Oracle Java SE Multiple Vulnerabilities (April 2013 CPU)	CVE-2013-0401	588
7	Oracle Java JDK/JRE Remote Code Execution Vulnerability	CVE-2013-0809	398
8	Apache 2.2 < 2.2.22 Multiple Vulnerabilities	CVE-2011-3368	349
9	Splunk Enterprise 6.4.2 Multiple Vulnerabilities	CVE-2013-0211	313
10	OpenSSL AES-NI Padding Oracle MitM Information Disclosure	CVE-2016-2107	296
11	Web Server Directory Traversal Arbitrary File Access	CVE-2000-0920	268
12	MS17-010: Windows SMB Remote Code Execution (EternalBlue)	CVE-2017-0143	252
13	MS08-067: Server Service Vulnerability	CVE-2008-4250	205
14	Microsoft Windows Unquoted Service Path Enumeration	CVE-2013-1609	192
15	Adobe Acrobat < 10.0.1 Multiple Vulnerabilities	CVE-2010-4091	189
16	OpenSSL Heartbeat Information Disclosure (Heartbleed)	CVE-2014-0160	186
17	Apache Tomcat / JBoss EJBInvokerServlet / JMXInvokerServlet Marshalled Object Remote Code Execution	CVE-2012-0874	167
18	PHP < 5.3.9 Multiple Vulnerabilities	CVE-2011-3379	165
19	MS15-004: Directory Traversal Elevation of Privilege Vulnerability	CVE-2015-0016	159
20	Adobe Reader < 9.1 Multiple Vulnerabilities	CVE-2009-0193	132
21	GNUC C Library < 2.23 Multiple Vulnerabilities	CVE-2015-7547	127
22	Mozilla Updater and Windows Update Service Privilege Escalation Vulnerability	CVE-2012-1942	119

23	MS10-096: Windows Address Book Insecure Library Loading Vulnerability	CVE-2010-3147	112
24	MS14-064: Windows OLE Automation Array Remote Code Execution Vulnerability	CVE-2014-6332	111
25	MS11-019: Browser Pool Corruption Vulnerability	CVE-2011-0654	101
26	MS11-026: MHTML Mime-Formatted Request Vulnerability	CVE-2011-0096	101
27	Sun Java Web Start JNLP Remote Code Execution Vulnerability	CVE-2007-3655	96
28	MS10-042: Vulnerability in Help and Support Center	CVE-2010-1885	95
29	MS10-097: Insecure Library Loading in Internet Connection Signup Wizard	CVE-2010-3144	95
30	MS11-003: Cumulative Security Update for Internet Explorer	CVE-2010-3971	92

NOTES:

In this table, we have only identified a single CVE ID for each vulnerability in order simplify our reporting.

Operating systems are not the only systems with exploitable vulnerabilities. Applications rank equally high.

- - - *Vulnerabilities: Top 30 Overall by Count (All Severity — External and Internal)*

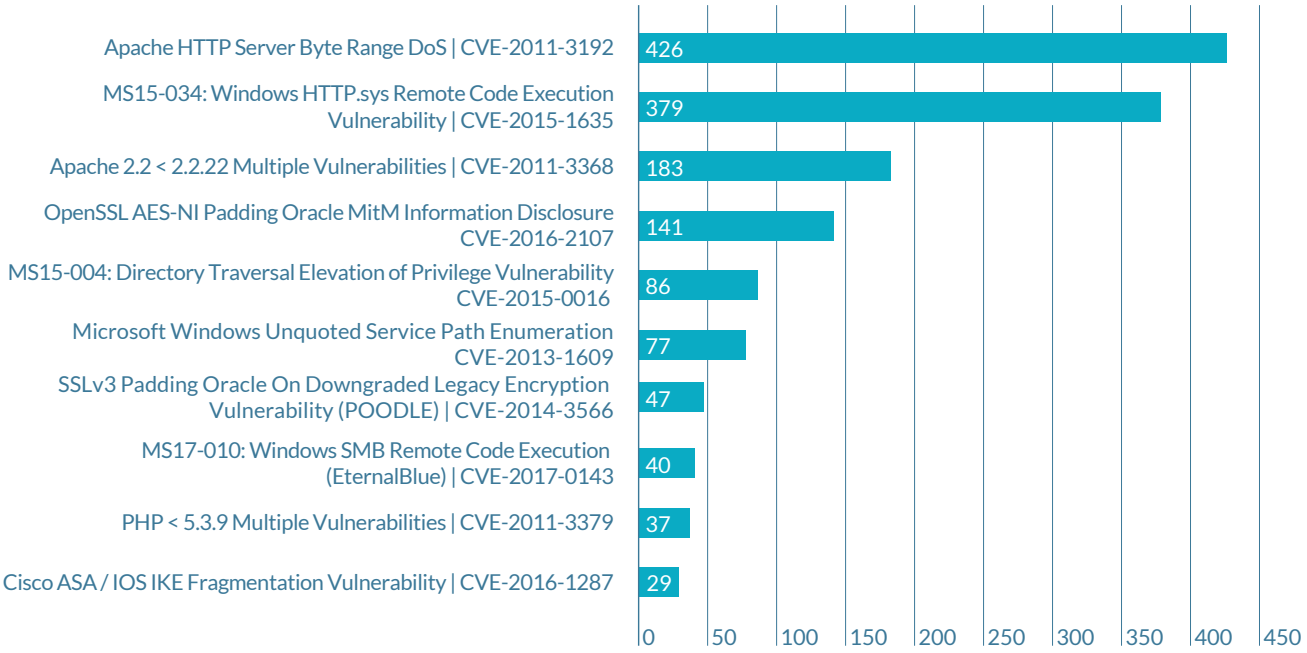
	Vulnerability	CVE ID	Count
1	Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	CVE-2005-1794	51450
2	SSL RC4 Cipher Suites Supported	CVE-2013-2566	43284
3	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	CVE-2014-3566	19237
4	SSH Server CBC Mode Ciphers Enabled	CVE-2008-5161	19201
5	SSL Certificate Signed Using Weak Hashing Algorithm	CVE-2004-2761	15131
6	Microsoft Windows SMB NULL Session Authentication	CVE-1999-0519	10216
7	SSL Version 2 (v2) Protocol Detection	CVE-2005-2969	5986
8	SSL / TLS Renegotiation Handshakes MiTM Plaintext Data Injection	CVE-2009-3555	5394
9	TLS Padding Oracle Information Disclosure Vulnerability (TLS POODLE)	CVE-2014-8730	4991
10	HTTP TRACE / TRACK Methods Allowed	CVE-2003-1567	4714
11	SSL/TLS Diffie-Hellman Modulus Weak Configuration (Logjam)	CVE-2015-4000	4347
12	Apache HTTP Server httpOnly Cookie Information Disclosure	CVE-2012-0053	3970
13	SNMP Agent Default Community Name (public)	CVE-1999-0517	3790
14	RomPager HTTP Referer Header XSS	CVE-2013-6786	3476
15	SSL 64-bit Block Size Cipher Suites Supported (SWEET32)	CVE-2016-2183	3246
16	Web Server HTTP Header Internal IP Disclosure	CVE-2000-0649	3094
17	MS12-020: Remote Desktop Protocol Vulnerability*	CVE-2012-0002	2836
18	SSH Protocol Version 1 Session Key Retrieval	CVE-2001-0361	2724
19	HP System Management Homepage < 7.0 Multiple Vulnerabilities	CVE-2009-0037	2058
20	MS14-066: Microsoft Schannel Remote Code Execution Vulnerability*	CVE-2014-6321	2018
21	MS16-047: Windows SAM and LSAD Downgrade Vulnerability (Badlock)*	CVE-2016-0128	2008
22	SSL/TLS EXPORT_RSA Weak Configuration (FREAK)	CVE-2015-0204	1937
23	Dropbear SSH Server < 2013.59, Multiple Vulnerabilities	CVE-2013-4421	1923
24	TLS CRIME Vulnerability	CVE-2012-4929	1908
25	SSL / TLS Renegotiation DoS	CVE-2011-1473	1654

* Uncredentialed check

26	Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	CVE-2002-1623	1540
27	Microsoft Windows Unquoted Service Path Enumeration	CVE-2013-1609	1430
28	Microsoft Windows Kernel Win32k.sys PATHRECORD chain Multiple Vulnerabilities	CVE-2013-3660	1398
29	MS15-034: Vulnerability in HTTP.sys Remote Code Execution	CVE-2015-1635	1364
30	MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Remote Code Execution	CVE-2010-3190	1237

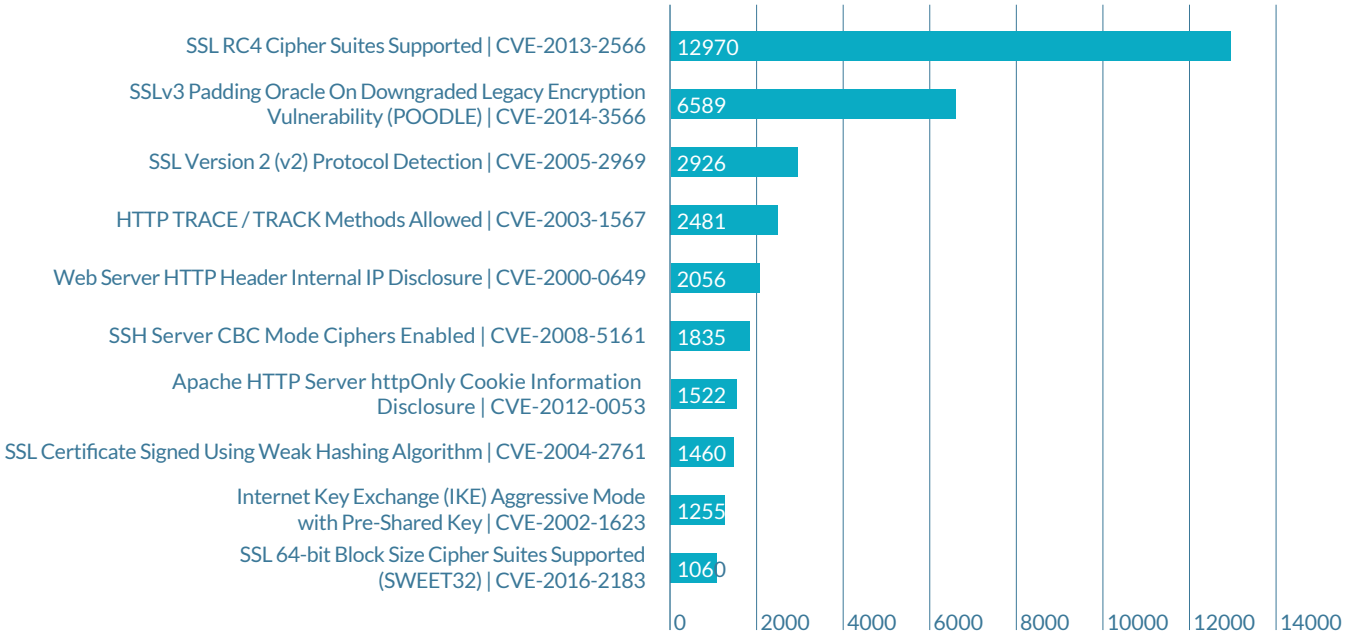
SSL vulnerabilities dominate the top 30 highest count.

Top 10 External Exploits



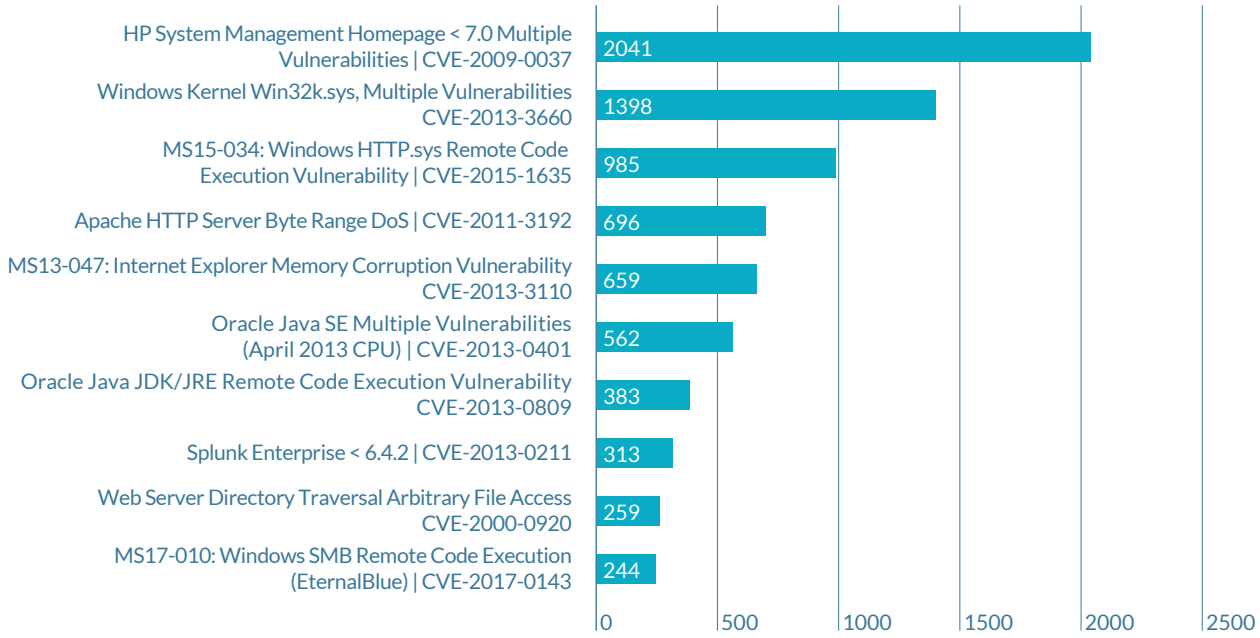
Missing Microsoft patch MS17-010, which WannaCry used as a transport method, cracked the list of top 10 external exploits in less than a year.

• • • *Top 10 External Vulnerabilities by Count*



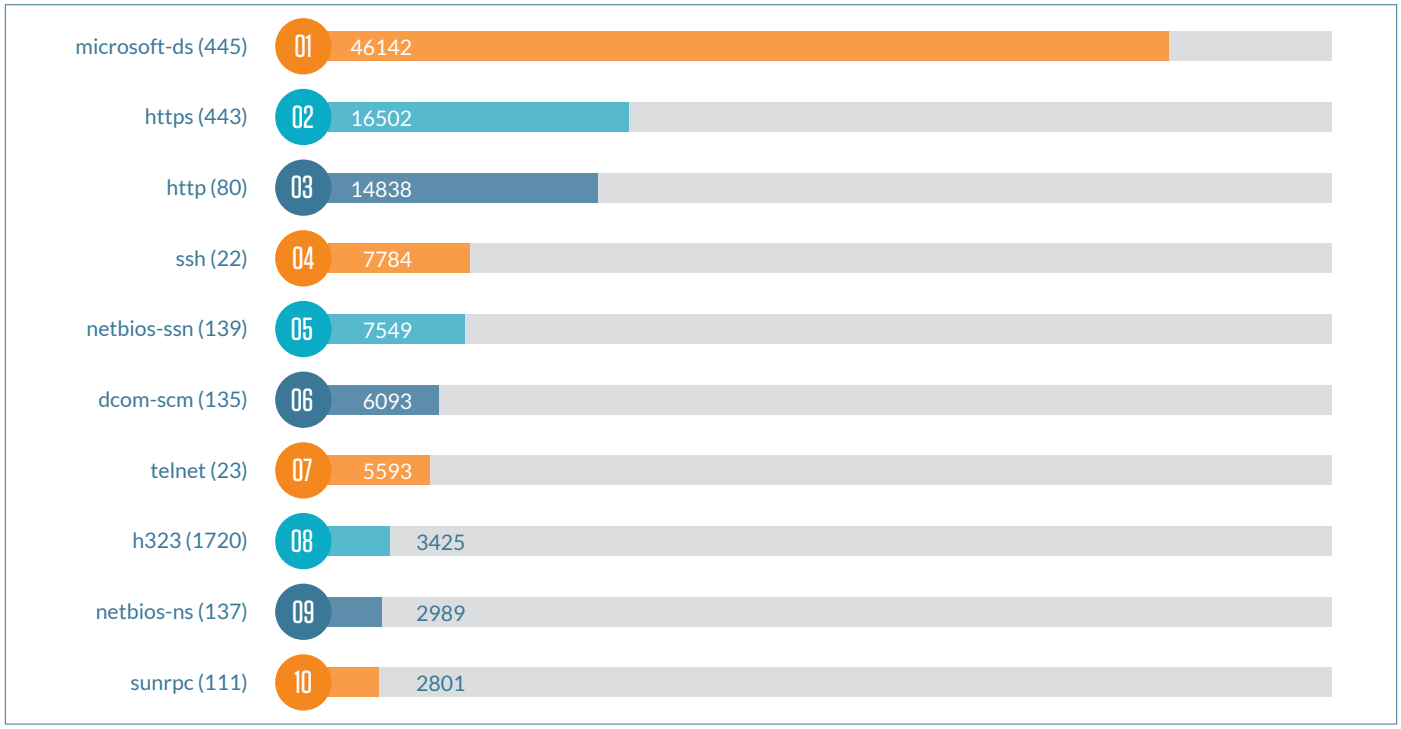
Most external vulnerabilities relate to web servers.

• • • *Top 10 Internal Exploits by Count*

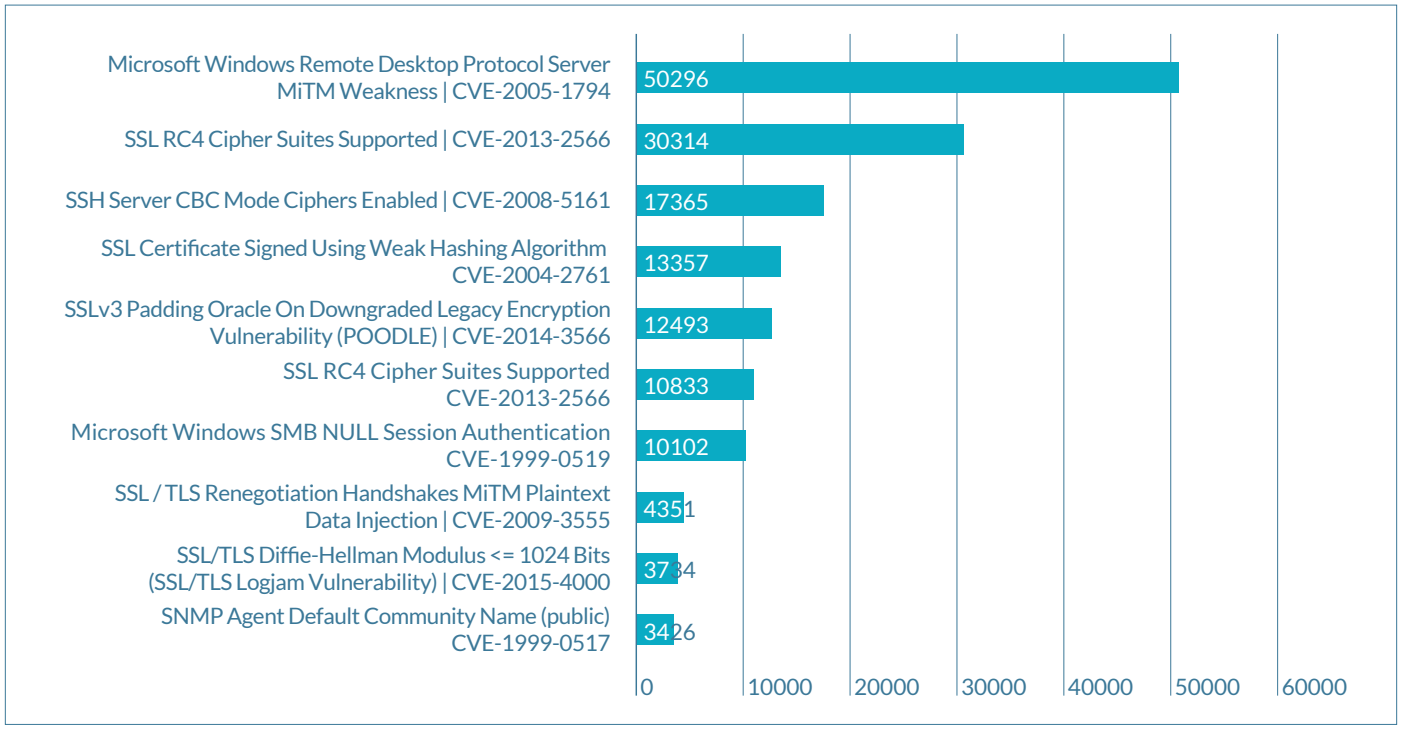


EternalBlue cracked the top 10 list of internal exploits by count, as well.

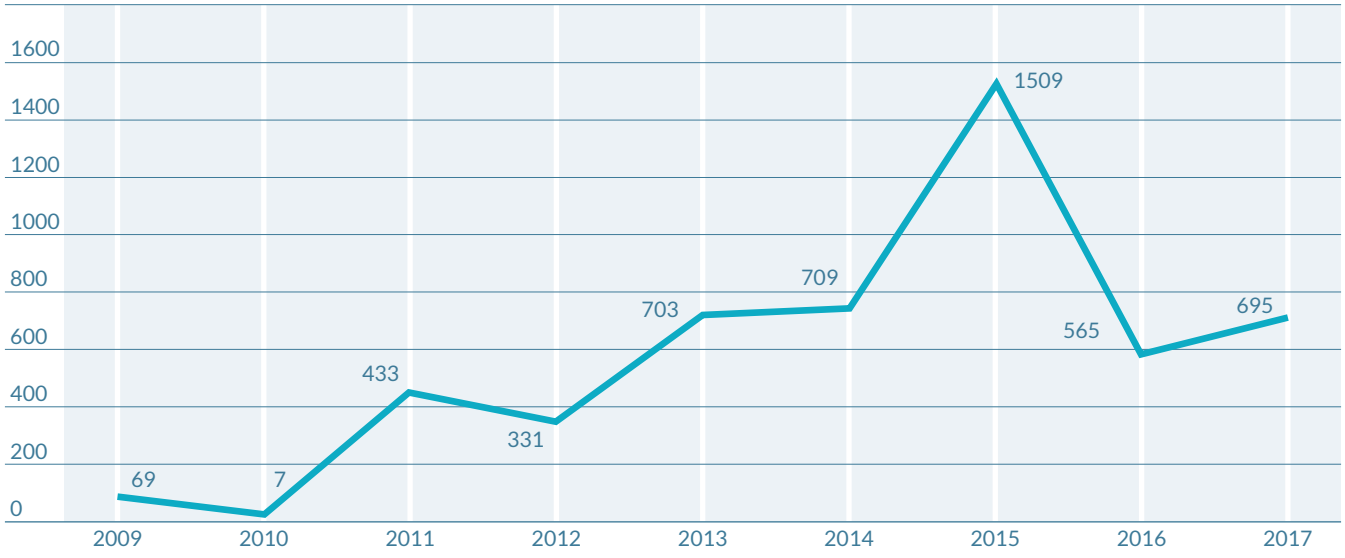
• • • *Top 10 Ports with Internal Vulnerabilities*



• • • *Top 10 Internal Vulnerabilities by Count*

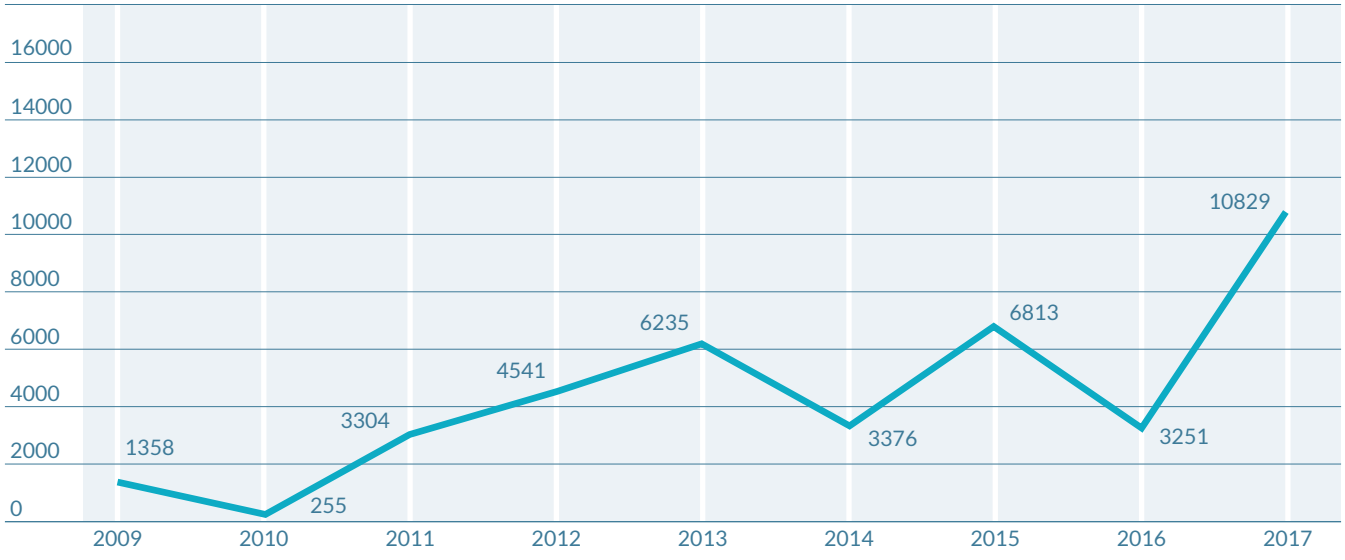


• • • *Total Exploits (External and Internal) Over Time*



In 2015, significant exploits included Adobe Flash and Microsoft Office vulnerabilities.

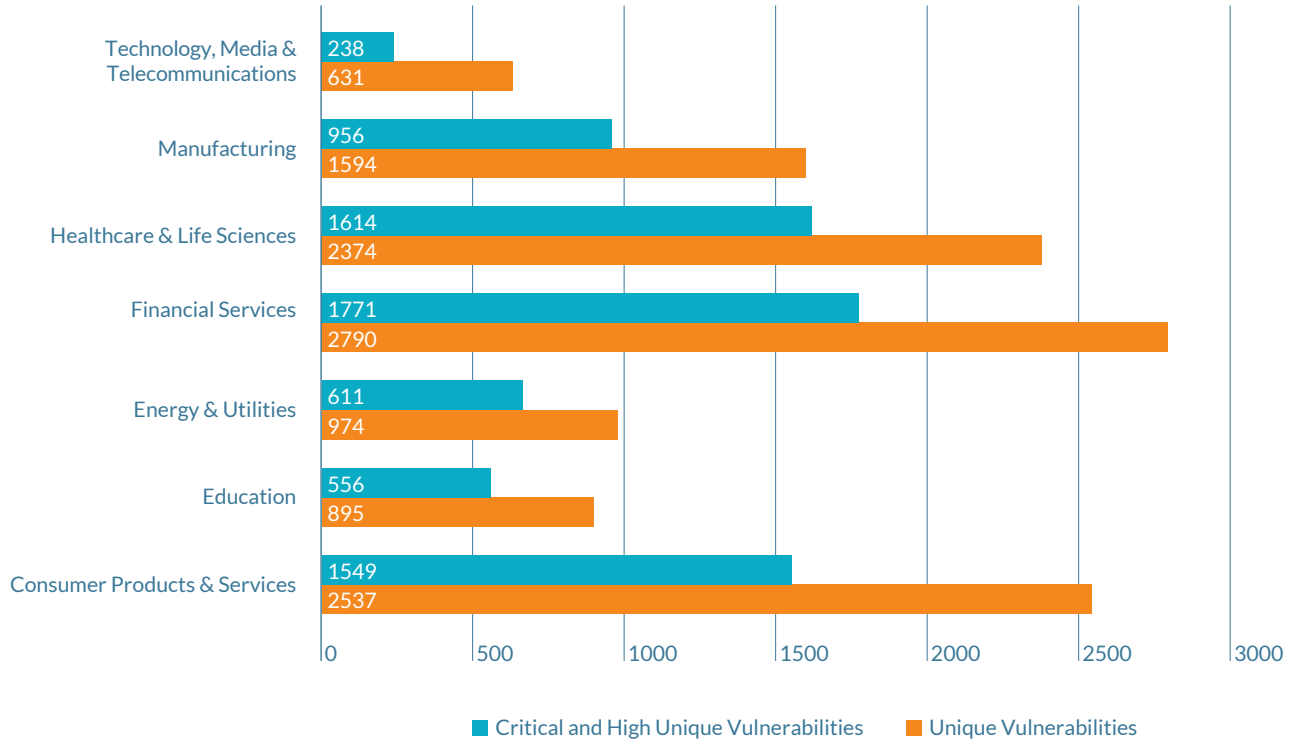
• • • *Total Vulnerabilities (External and Internal) Over Time*



As expected, the number of vulnerabilities identified over time is increasing.

Overall Industry Findings (2009 – 2017)

• • • *Vulnerability Severity by Industry*



Technology, Media and Telecommunications organizations had the lowest percentage of vulnerabilities that were "critical" or "high" in severity.

NOTES:
Organizations included by industry and number of scans/tests performed: Consumer Products & Services 36%, Financial Services 29%, Healthcare & Life Sciences 10%, Technology, Media & Telecommunications 9%, Manufacturing 8%, Energy & Utilities 7%, Education 1%.

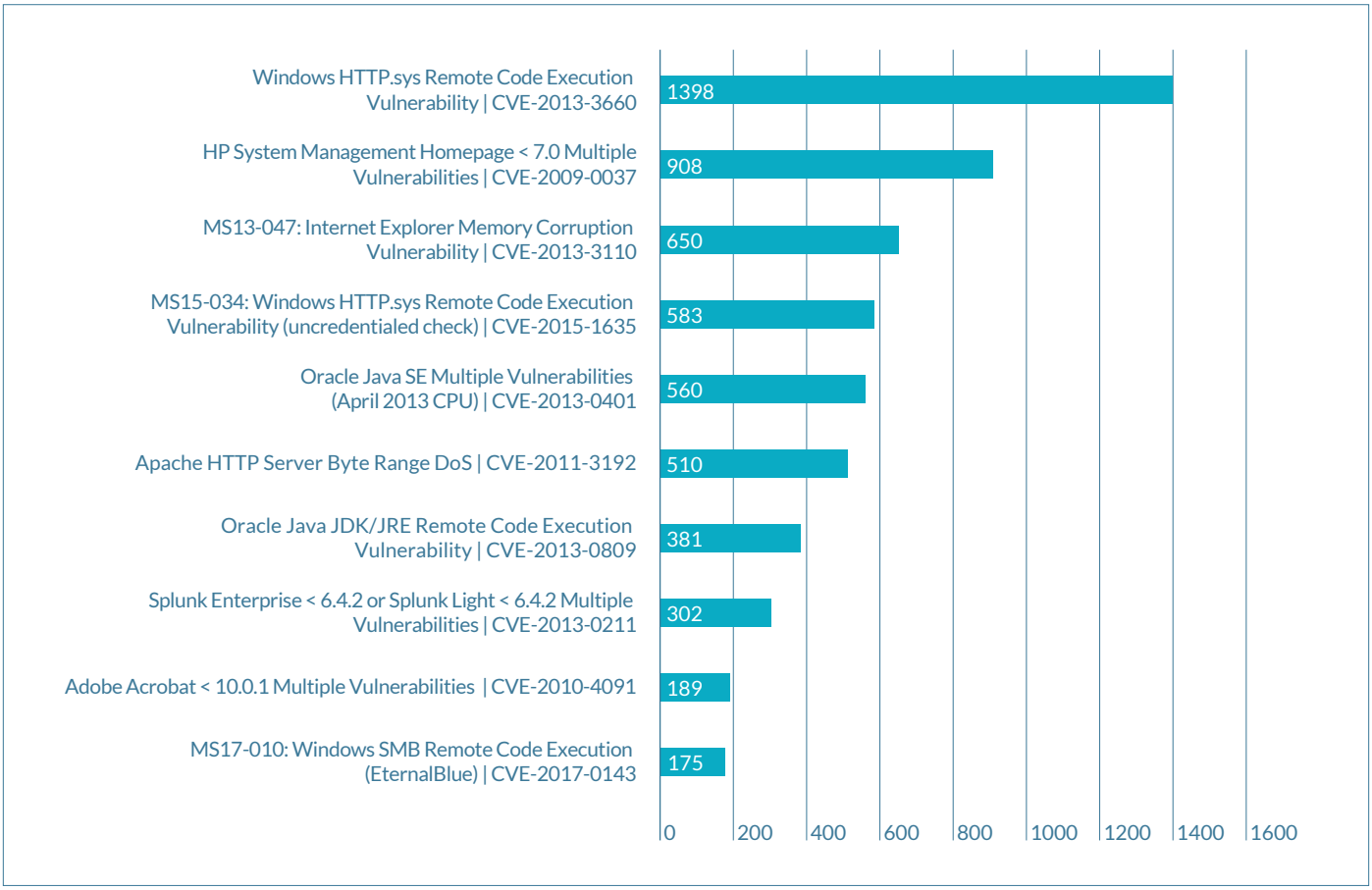
• • • *Exploits by Industry*

By their very nature, most exploits are considered "critical" or "high" in severity.

NOTES:
Organizations included by industry and number of scans/tests performed: Consumer Products & Services 36%, Financial Services 29%, Healthcare & Life Sciences 10%, Technology, Media & Telecommunications 9%, Manufacturing 8%, Energy & Utilities 7%, Education 1%.

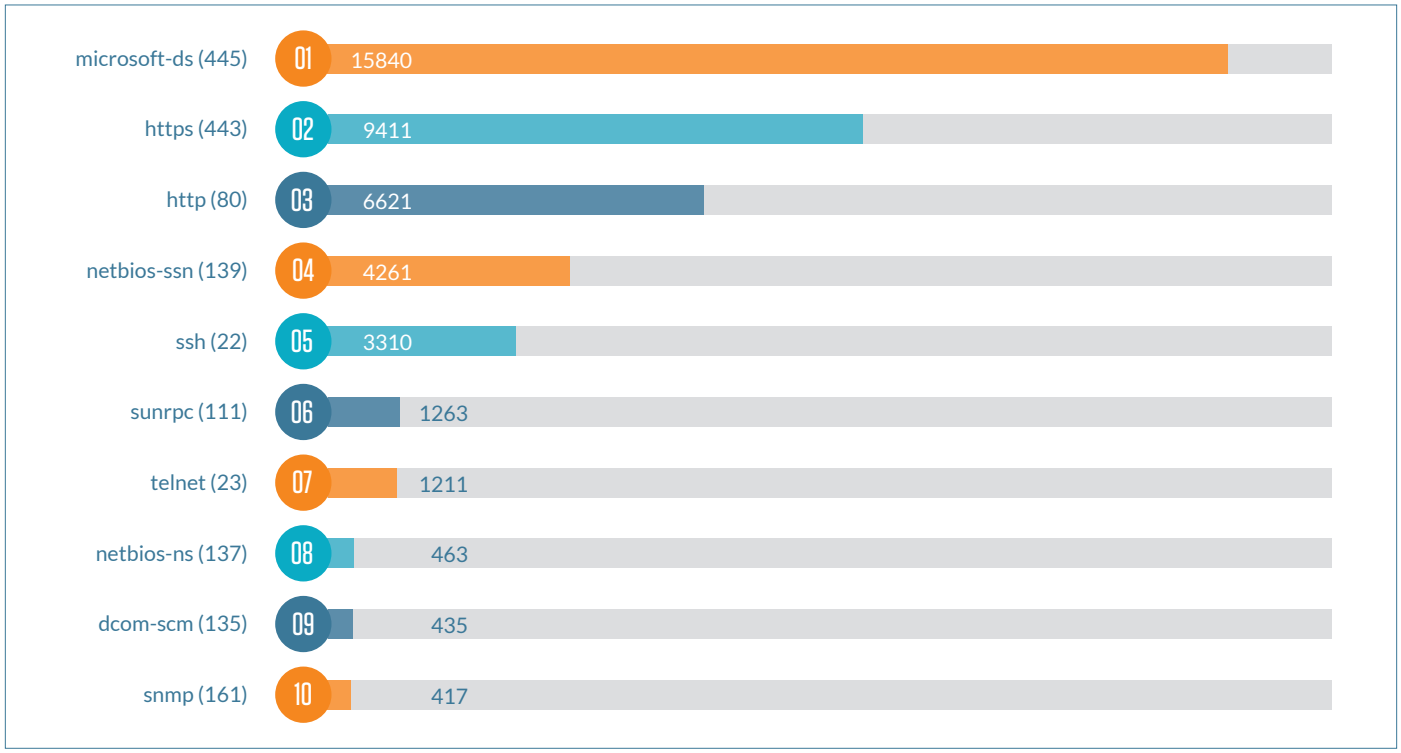
Financial Services

• • • *Top 10 Overall Exploits (External and Internal)*



Financial Services (cont.)

- *Top 10 Overall Exploits by Port (External and Internal)*



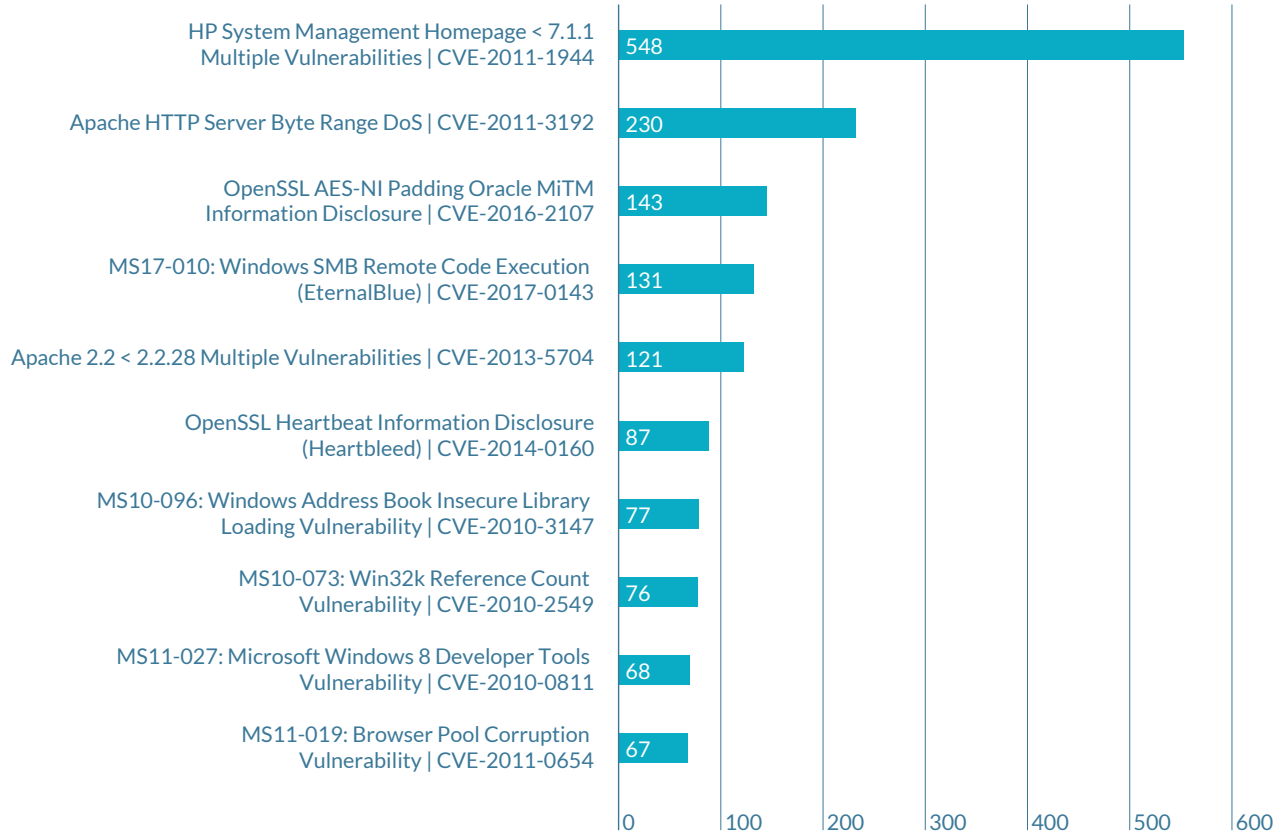
Financial Services (cont.)

- *Top 10 Overall Vulnerabilities (External and Internal)*

Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	**17608**
SSL RC4 Cipher Suites Supported	**9253**
SSH Server CBC Mode Ciphers Enabled	**5662**
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	**5451**
Microsoft Windows SMB NULL Session Authentication	**3575**
HTTP TRACE / TRACK Methods Allowed	**2169**
SSL Version 2 Protocol Detection	**1967**
Apache HTTP Server httpOnly Cookie Information Disclosure	**1779**
RomPager HTTP Referer Header XSS	**1705**
Microsoft Windows Kernel Win32k.sys PATHRECORD chain Multiple Vulnerabilities	**1398**

Consumer Products and Services

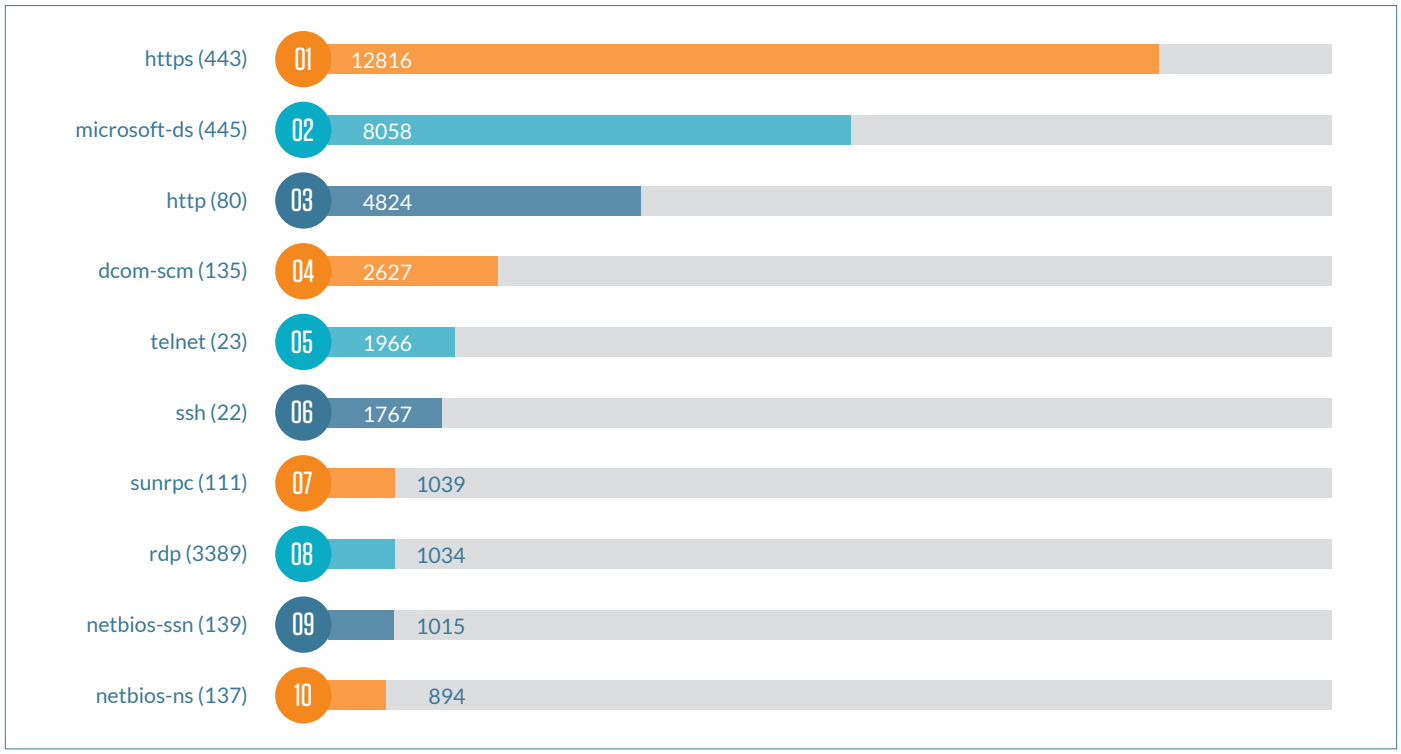
• • • *Top 10 Overall Exploits (External and Internal)*



Consumer Products and Services organizations had more MS17-010 exploits identified than other industries.

Consumer Products and Services (cont.)

- *Top 10 Overall Exploits by Port (External and Internal)*



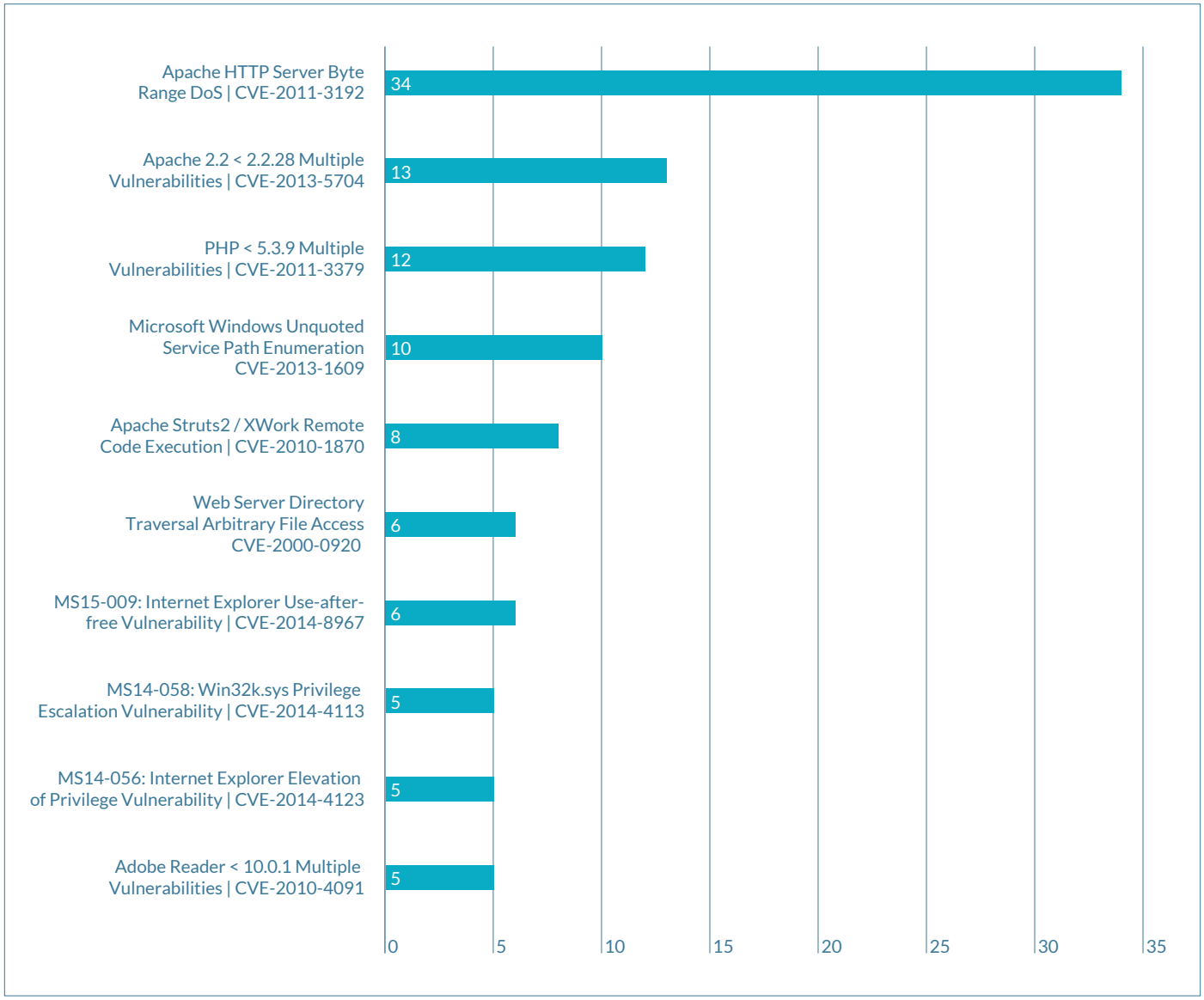
Consumer Products and Services (cont.)

- *Top 10 Overall Vulnerabilities (External and Internal)*

Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	9342
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	6003
SSL Certificate Signed Using Weak Hashing Algorithm	5461
SSH Server CBC Mode Ciphers Enabled	4008
SSL Version 2 Protocol Detection	1781
Web Server HTTP Header Internal IP Disclosure	1579
Microsoft Windows SMB NULL Session Authentication	1385
HTTP TRACE / TRACK Methods Allowed	948
Apache HTTP Server httpOnly Cookie Information Disclosure	880
SNMP Agent Default Community Name	817

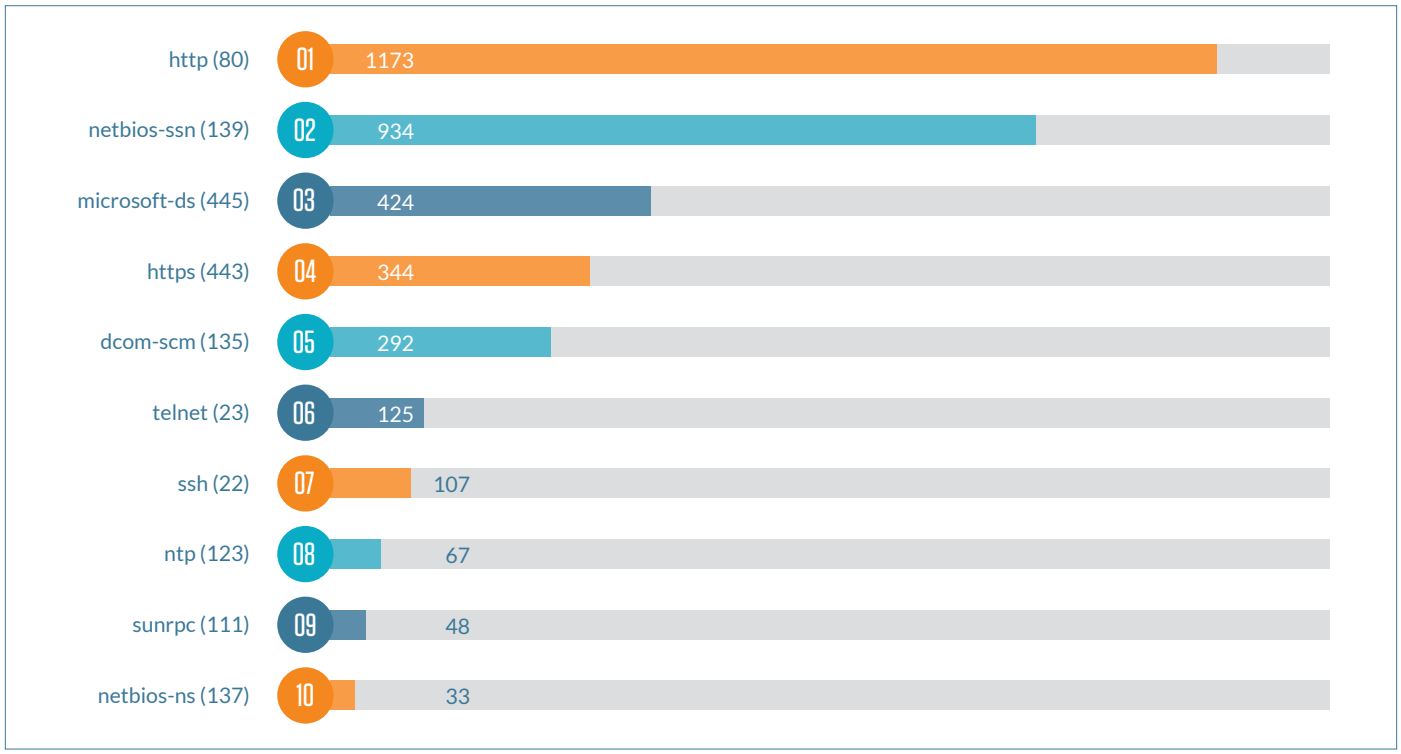
Education

• • • *Top 10 Overall Exploits (External and Internal)*



Education (cont.)

- *Top 10 Overall Exploits by Port (External and Internal)*



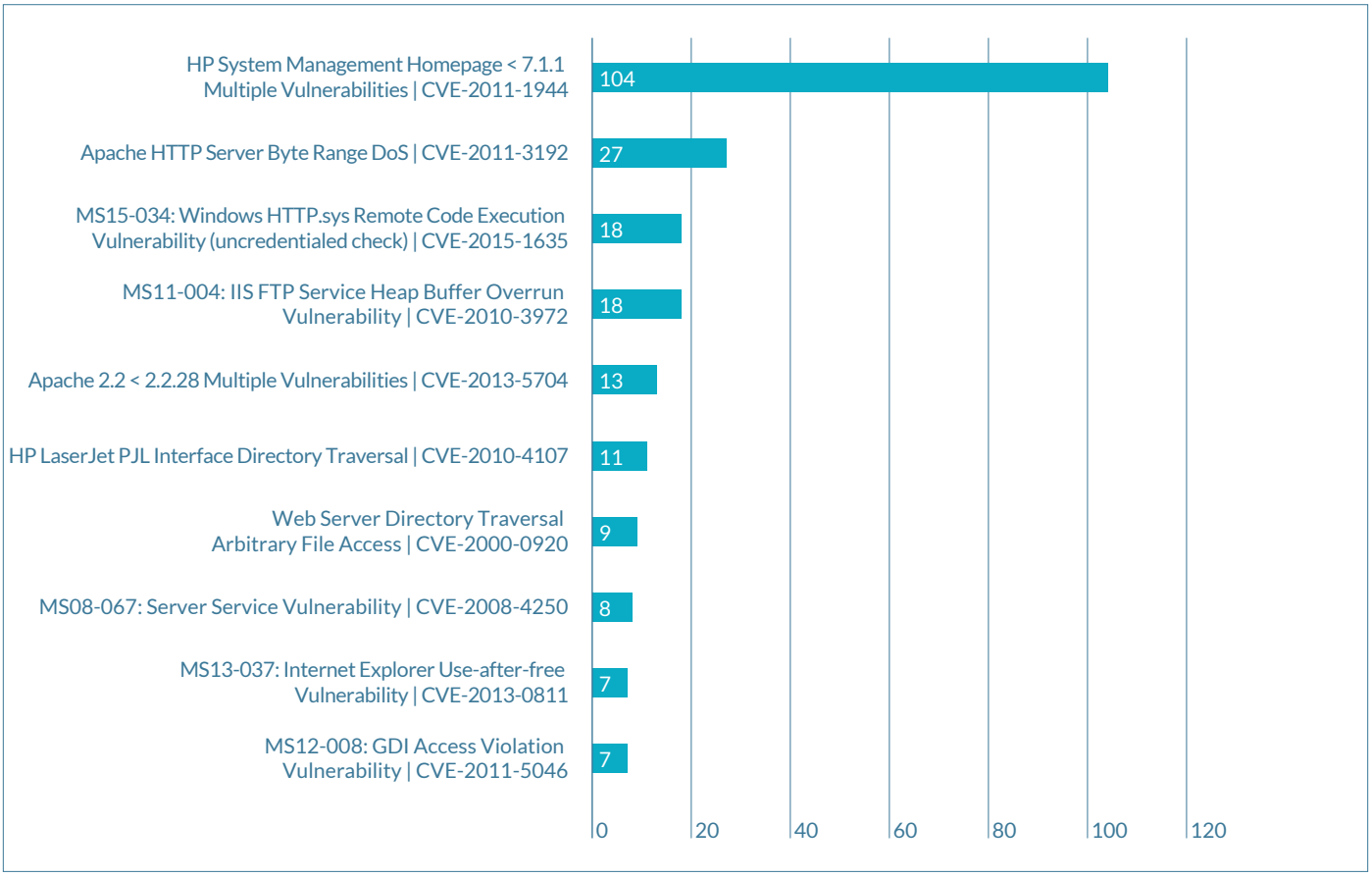
Education (cont.)

- *Top 10 Overall Vulnerabilities (External and Internal)*

SSL RC4 Cipher Suites Supported	948
Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	426
HTTP TRACE / TRACK Methods Allowed	241
Apache HTTP Server httpOnly Cookie Information Disclosure	193
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	163
SSL Version 2 Protocol Detection	107
Microsoft Windows SMB NULL Session Authentication	84
SNMP Agent Default Community Name	61
Web Server Generic XSS	37
Apache HTTP Server Byte Range DoS	34

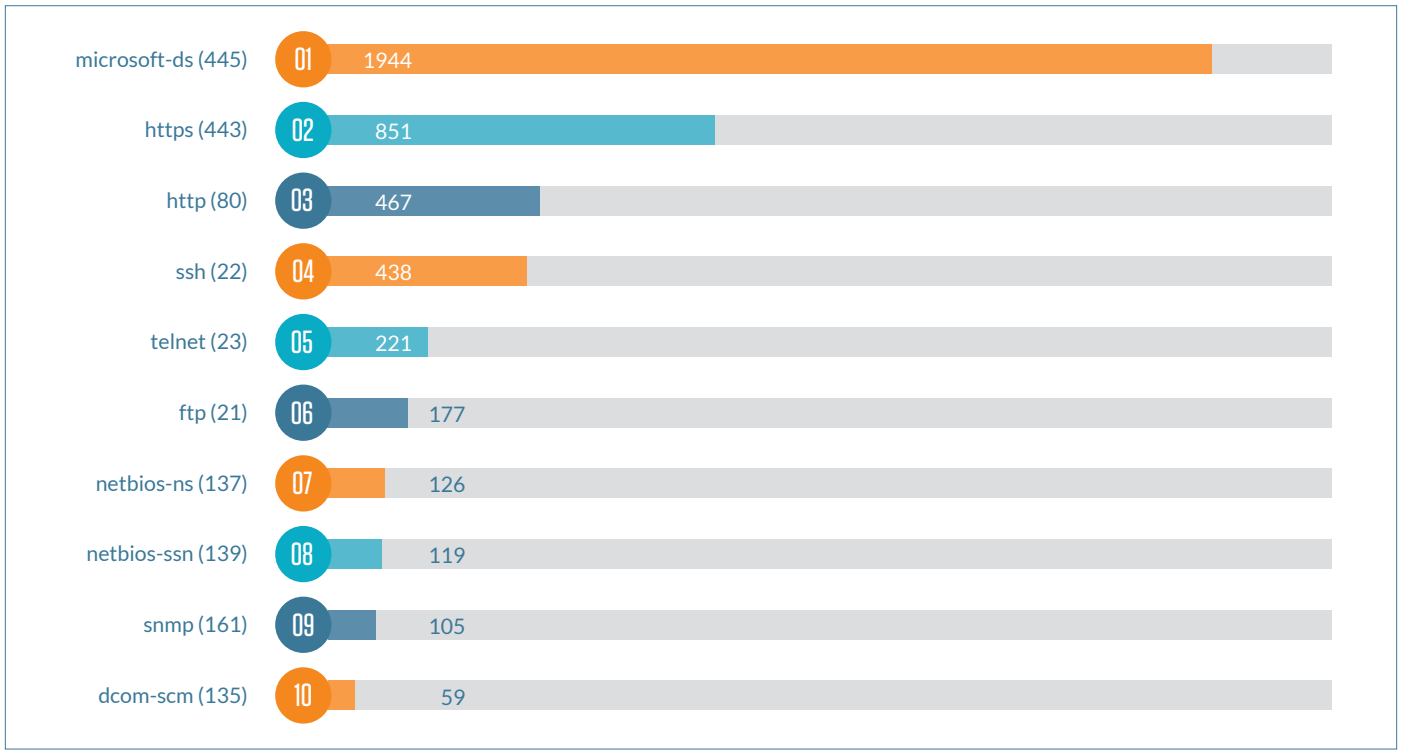
Energy and Utilities

- - - *Top 10 Overall Exploits (External and Internal)*



Energy and Utilities (cont.)

• • • *Top 10 Overall Exploits by Port (External and Internal)*



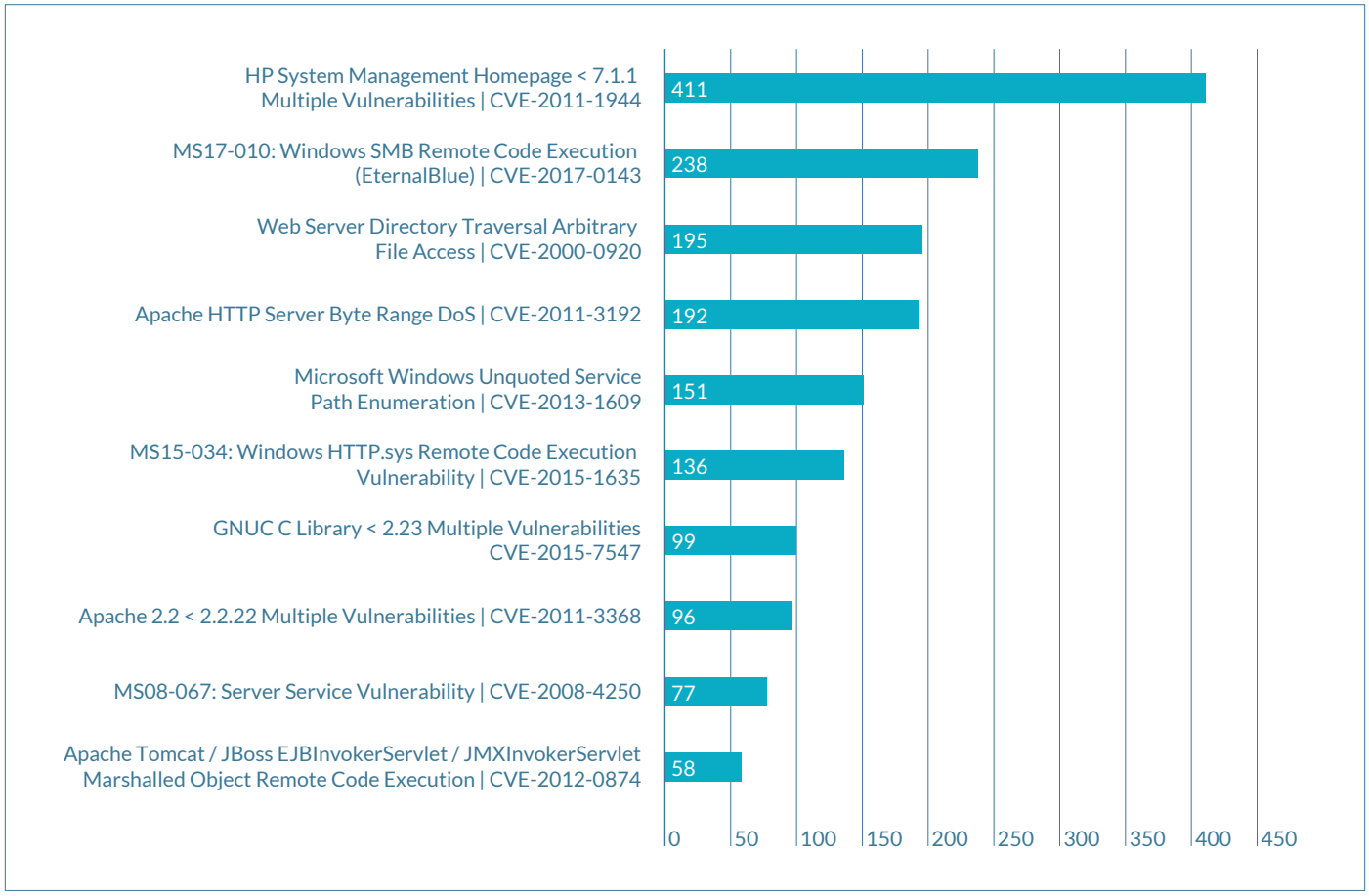
Energy and Utilities (cont.)

• • • *Top 10 Overall Vulnerabilities (External and Internal)*

SSL RC4 Cipher Suites Supported	2275
Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	1801
SSH Server CBC Mode Ciphers Enabled	999
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	488
SSL Version 2 Protocol Detection	351
SNMP Agent Default Community Name	332
Microsoft Windows SMB NULL Session Authentication	267
RomPager HTTP Referer Header XSS	199
SSH Protocol Version 1 Session Key Retrieval	181
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution	148

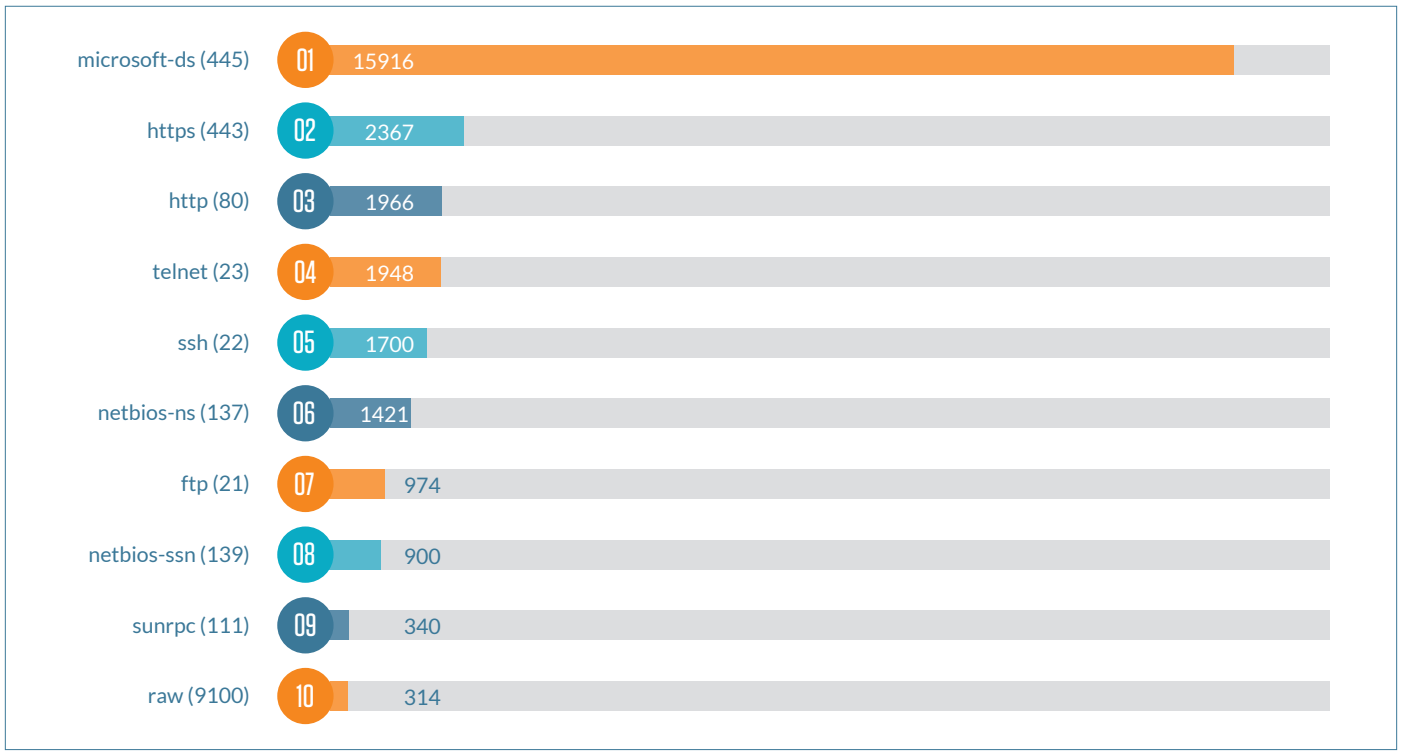
Healthcare and Life Sciences

• • • *Top 10 Overall Exploits (External and Internal)*



Healthcare and Life Sciences (cont.)

• • • *Top 10 Overall Exploits by Port (External and Internal)*



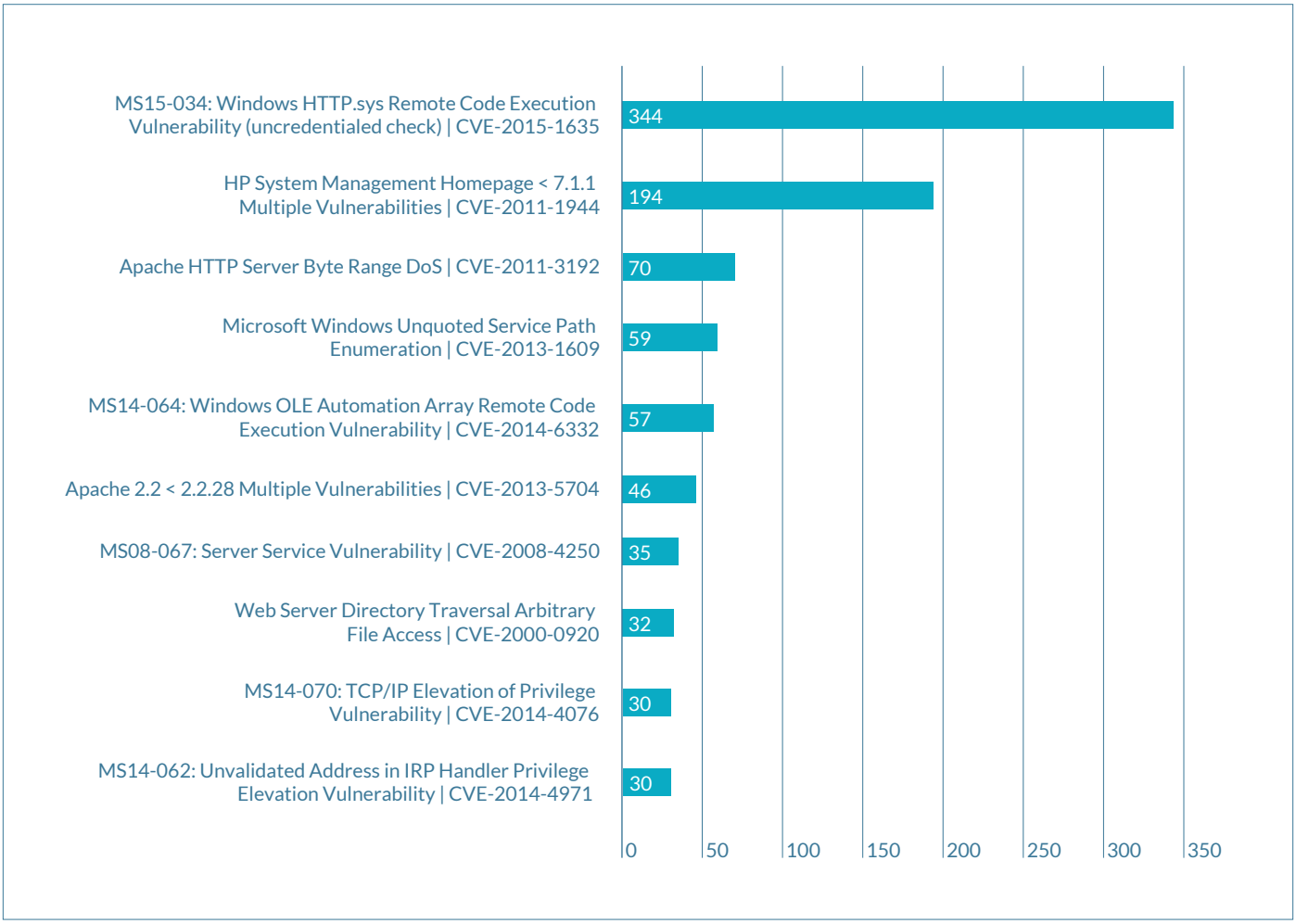
Healthcare and Life Sciences (cont.)

- *Top 10 Overall Vulnerabilities (External and Internal)*

Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	15721
SSL RC4 Cipher Suites Supported	14456
SSH Server CBC Mode Ciphers Enabled	5786
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	3992
Microsoft Windows SMB NULL Session Authentication	3092
Dropbear SSH Server < 2013.59 Multiple Vulnerabilities	1211
MS16-047: Security Update for SAM and LSAD Remote Protocols	936
SNMP Agent Default Community Name	760
SSL Version 2 Protocol Detection	596
Chargen UDP Service Remote DoS	530

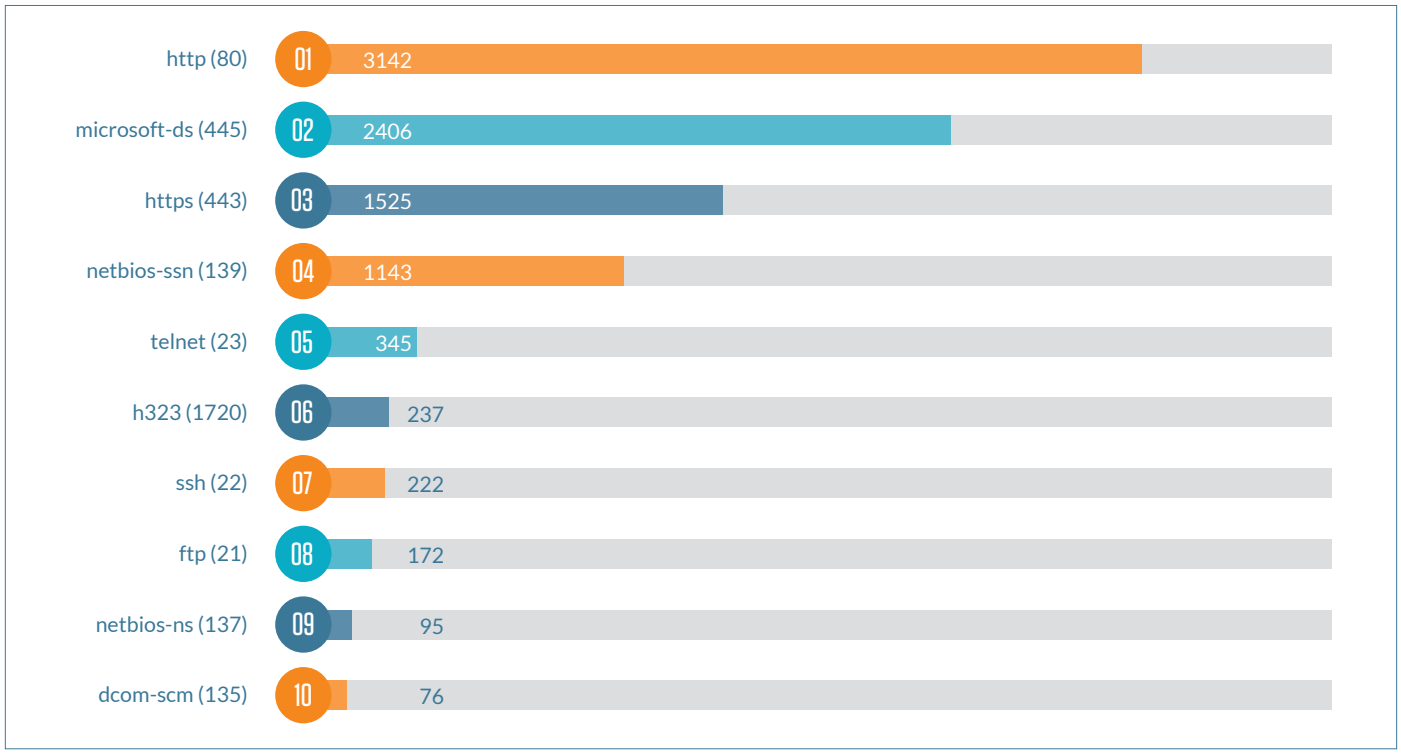
Manufacturing

• • • *Top 10 Overall Exploits (External and Internal)*



Manufacturing (cont.)

• • • *Top 10 Overall Exploits by Port (External and Internal)*



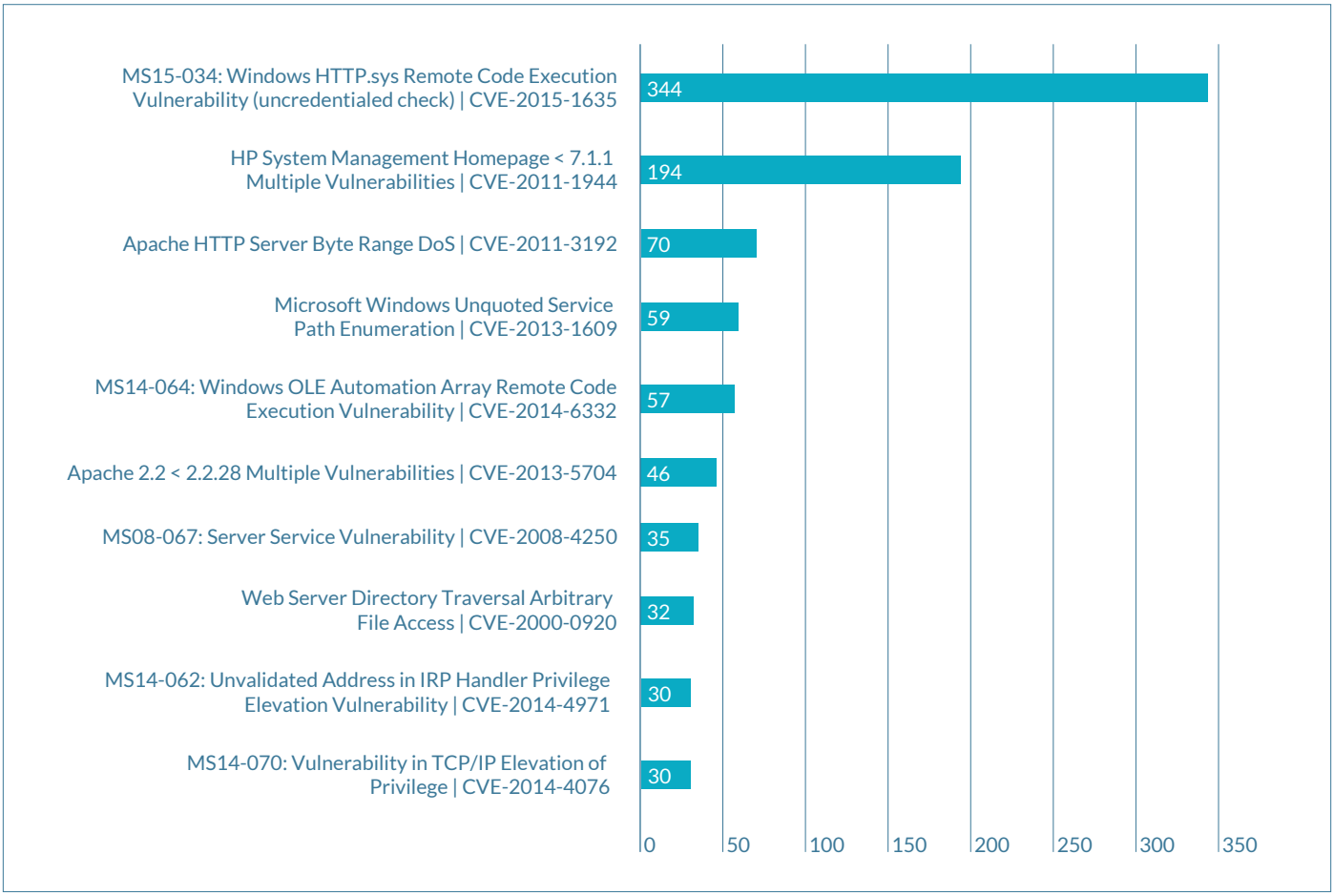
Manufacturing (cont.)

- *Top 10 Overall Vulnerabilities (External and Internal)*

Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	3192
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	2147
SSL RC4 Cipher Suites Supported	1925
RomPager HTTP Referer Header XSS	1481
SSH Server CBC Mode Ciphers Enabled	1329
Microsoft Windows SMB NULL Session Authentication	1267
MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution	581
SNMP Agent Default Community Name	505
HTTP TRACE / TRACK Methods Allowed	384
MS14-066: Vulnerability in Schannel Could Allow Remote Code Execution	365

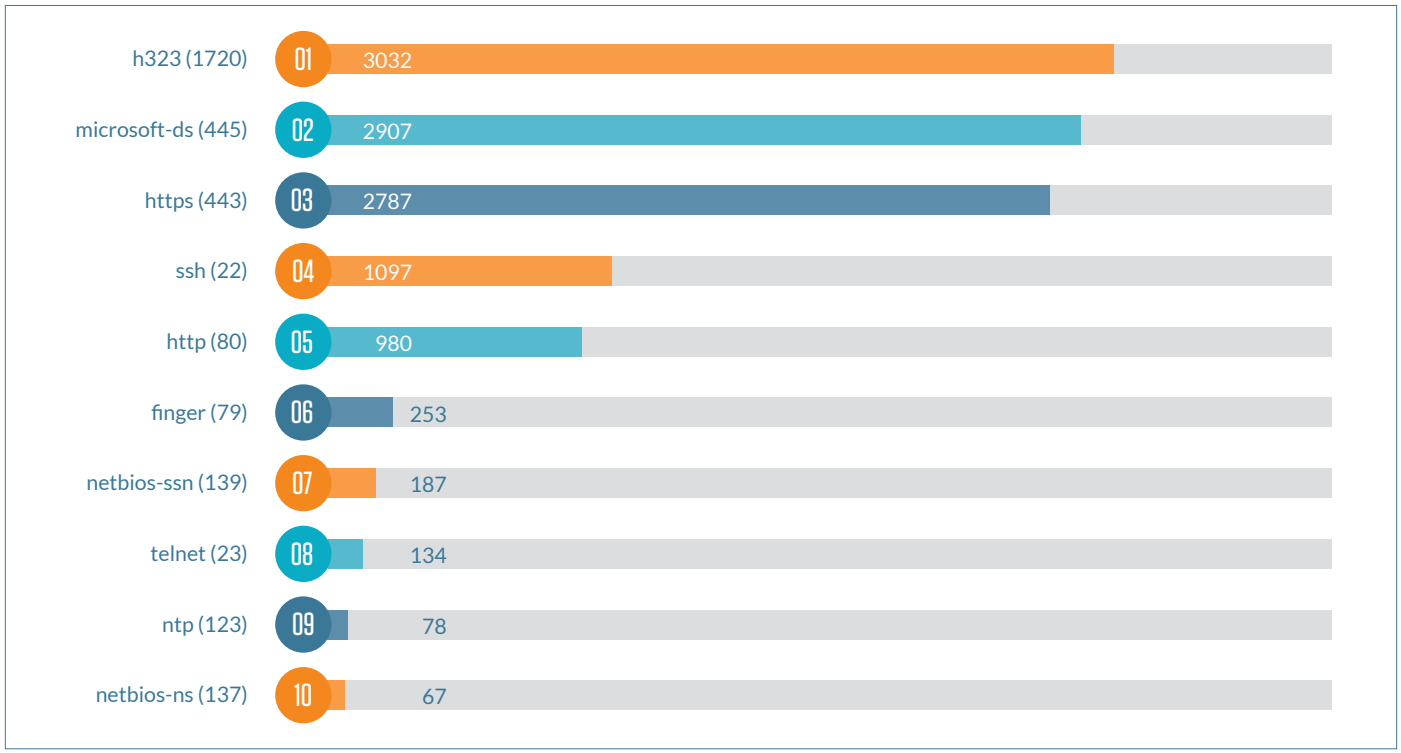
Technology, Media and Telecommunications

• • • *Top 10 Overall Exploits (External and Internal)*



Technology, Media and Telecommunications (cont.)

- - - *Top 10 Overall Exploits by Port (External and Internal)*



Technology, Media and Telecommunications (cont.)

- *Top 10 Overall Vulnerabilities (External and Internal)*

SSL RC4 Cipher Suites Supported	4840
Microsoft Windows Remote Desktop Protocol Server MiTM Weakness	1673
SSH Server CBC Mode Ciphers Enabled	1087
SSL Version 2 Protocol Detection	874
SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	787
Web Server HTTP Header Internal IP Disclosure	738
Microsoft Windows SMB NULL Session Authentication	496
HTTP TRACE / TRACK Methods Allowed	420
Apache HTTP Server httpOnly Cookie Information Disclosure	226
Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key	208

Key Questions to Consider

Following are some suggested questions that CIOs and IT leaders should consider, based on the context of and risks inherent in the entity's operations:

- Are our systems correctly configured to prevent hackers from getting in?
- Does our organization have a good handle on its asset inventory? Specifically, do we know what's exposed on the internet and what's not? Is it protected?
- Are we protected from insider threats?
- Are web applications developed and maintained in a manner to resist attack?
- Do our employees know how to identify and respond to attacks?

Final Thoughts

Over the past decade, the cyber threat landscape clearly has been perilous for organizations and undoubtedly will remain so in the years ahead. What can organizations learn from all of this? Perhaps the key lesson is that any organization most likely has security vulnerabilities in one or more areas. To understand these vulnerabilities better, organizations should perform a comprehensive assessment to identify their security vulnerabilities and threats. Further, the calls to action detailed earlier provide a roadmap for organizations to improve their overall security posture.

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Kurt Underwood
Managing Director
Global Leader, Technology Consulting Practice
+1.206.262.8389
kurt.underwood@protiviti.com

Scott Laliberte
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

Andrew Retrum
Managing Director
+1.312.476.6353
andrew.retrum@protiviti.com

Randy Armknecht
Managing Director
+1.312.476.6428
randy.armknecht@protiviti.com

Michael Walter
Managing Director
+1.303.898.9145
michael.walter@protiviti.com

Tom Stewart
Director
+1.312.931.8901
tom.stewart@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Indianapolis
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE
Paris

GERMANY
Frankfurt
Munich

ITALY
Milan
Rome
Turin

NETHERLANDS
Amsterdam

UNITED KINGDOM
London

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

INDIA*
Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

protiviti®