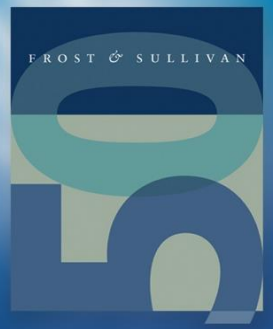
Analysis of the Global Public Vulnerability Research Market, 2015

Growth of Public Vulnerability Disclosures, the Important Intermediary Between Commercial Threat Analysis and Cyber Grid Threat Reporting



K116-74

October 2016

FROST & SULLIVAN

Research Team

Lead Analyst

Tony Massimini
Industry Analyst
ICT – Network Security

(602) 301-7485
Tony.Massimini@frost.com

Contributing Analyst

Chris Kissel
Industry Analyst
ICT – Network Security

(623) 910-7986
Christopher.Kissel@frost.com

Vice President of Research

Michael Suby
VP of Research
Stratecast/Frost & Sullivan

(303) 946-2407
Mike.suby@frost.com

Contributing Analyst

Chris Rodriguez
Industry Analyst
ICT – Network Security

(210) 477-8423
Chris.Rodriguez@frost.com

Table of Contents

Executive Summary

Executive Summary—Key Findings

- The organizations that are vulnerability-disclosing institutions used within this report include:
  - Core Security, Fortinet, Google Project Zero, High-Tech Bridge, IBM, Secunia, US-CERT, Trend Micro Zero Day Initiative (inclusive of the company's acquisition of TippingPoint from HP), and Verisign.
  - Government reporting refers to vulnerabilities disclosed by the United States Computer Emergency Readiness Team (US-CERT).
    - The US-CERT is a government agency, but the other reporting organizations either sell security-related services or sell security devices.
- Frost & Sullivan considers vulnerabilities that have been disclosed by public vulnerability reporting agencies—this pool of vulnerabilities totals 1,337 in 2015, a 43.8% increase from 2014, with the top three reporting agencies being:
  - Trend Micro ZDI had 656 verified, publicly reported vulnerabilities
  - Google Project Zero reported 302 vulnerabilities
  - US-CERT had 219 vulnerabilities

Source: Frost & Sullivan analysis.

Market Overview

Market Overview

- The following is both a study about software vulnerabilities and the companies that publicly disclose vulnerabilities.
- A security vulnerability is any error in an IT system that can be exploited by an attacker to compromise the confidentiality or integrity of a system or to deny legitimate user access to a system. Other industry terms for security vulnerabilities include “software bug” and “flaw.”
- In the past, the process by which the analysis of vulnerabilities was shared with third parties was subject to much debate, as full disclosure is the practice of making the details of security vulnerabilities public. Public vulnerability disclosures have many different stakeholders including:
  - **The companies affected.** As an example, a vulnerability is discovered within a CIGNA customer relationship management (CRM) platform. Ideally, before the incident went public, the software would be patched and the public disclosure would be made in a perfect world. However, there are several reasons that CIGNA (again this is an example) would be reticent to allow a public disclosure. Those reasons are:
    - While a patch may be vulnerability-specific, it also shows where a successful vulnerability occurred. If a patch was applied to a vulnerability in a LINUX kernel, it stands to reason that an educated hacker would make a precursory examination to see if there were other ways to exploit the kernel.
    - If a vulnerability is disclosed and patched, unfortunately in a de facto fashion, the company admits there was a vulnerability in the first place. In many vertical markets, non-compliance, even if reasonable precautions are taken, still can bring forth a fine. The U.S Department of Health and Human Service (HHS), Office for Civil Rights, can levy fines of as little as $100 to as much as $1.5 million for security breaches. Even $100 incidents could have cascading effects as a single breach potentially affects multiple systems or patients.
    - Indemnity becomes a factor. If an end user can prove that his assets or his personally identifiable information (PII) was disclosed between the time a vulnerability was discovered against the time that the vulnerability was patched, conceivably there is a possible matter of compensation for the end user.
    - No matter how well-intended or enlightened a company is, no one likes to admit a flaw or error.

Source: Frost & Sullivan analysis.

Market Overview (continued)

- **The public disclosing entity.** The public disclosing entity has to manage many moving parts. On the most simplistic level, the disclosing company has to dedicate resources to the proper posting of vulnerabilities and the responsibilities of double-checking. Importantly, the company with the intent of disclosing a vulnerability has a fiduciary responsibility to give the Product Security Incident Response Team (PSIRT) of the companies with the vulnerabilities ample time to mitigate the threat and patch the vulnerability.
- **Individual contributors.** In many of the public vulnerability programs, individuals disclosing vulnerabilities receive notoriety and in the majority of cases receive a financial reward. In terms of compensation for the individual contributor, a public disclosing company gives greater rewards for higher vulnerability scores, the type of applications affected, and the clarity with which the vulnerability disclosure is written (i.e., if independent researchers can use the same methodology as the ethical hackers did and achieve the same result). However, increasingly, individual contributors are finding other revenue streams by working through privately-hosted "bug bounty" programs which we discuss later in the report.

- Organizations tend to treat vulnerabilities less as a software problem and more as a public relations (PR) problem.
- All of these concerns are valid, and in spite of them, Frost & Sullivan still sees the need for public vulnerability disclosure.
- In the first place, the existence of public vulnerability disclosure creates a layer of accountability and transparency for individual companies affected, Web hosting and applications providers, and software providers who may not be practicing due diligence as far as writing secure code are put on notice—full disclosure comes into play by making the PR problem more acute, organizations are then quicker to patch vulnerabilities.
- Secondly, formal public vulnerability disclosure has helped to shape the standardization of how vulnerabilities are tracked, managed and stored.

Source: Frost & Sullivan analysis.

Market Overview (continued)

- Lastly, hacker sophistication is growing exponentially. A miscreant may create a bot that detonates when detected, or automatically encrypts information when sending back to a command and control (C&C) server, or may lay dormant for a period of times as in a zero-day threat.
- Conventional vulnerability assessment tools can only go so far toward discovering the threat exposure surface.
- The continued existence of public vulnerability programs achieves these initiatives:
  - Demonstrates a seriousness in the treatment of threat exposure data. For example, Trend Micro ZDI can point to TippingPoint and demonstrate how its findings are directly leveraged into its threat detection and response platforms. Google started Project Zero, in part, so that its end users can be assured that Google is doing all it can to provide a safe environment for the users of its browsers, its keyword searches, and its Apps Store.
  - Keeps vendors enterprise network practitioners, application providers, and software developers on their toes—offers a degree of attestation (whether wanted or not).
  - Public disclosure is the natural midpoint of two larger security forces. On one hand, there is private cyber security companies like FireEye or Palo Alto Networks reporting threat data directly to their clients (private entity-to-private entity communication). On the other hand there is an evolving open-standards framework involving Trusted Automated Exchange of Indicator Information (TAXII), Cyber Observable Expression (CybOX) and Structured Threat Information Expression (STIX), for the sharing of threat discovering and information sharing. Public disclosure reporting is and can continue to be an asset to both.

Source: Frost & Sullivan analysis.

Bug Bounty Programs and Contests

- Public vulnerability disclosure is not the only type of way to receive contributions form individual contributors.
- One way to crowdsource enthusiasts is to sponsor open competitions. TippingPoint has held the Pwn2Own competition since 2007 (see next page).
- From 2010–2014, Google staged GooglePwnium contests. In 2015, Google scrapped the annual competition in preference to a year-round Chrome Vulnerability Reward Program. Through February 2015, Google said it paid over $4 million in bug bounty rewards.
- Several companies offer continuous bug bounty programs. The most visible companies with bug bounty programs include Facebook, Firefox/Mozilla, Google, Microsoft, and Yahoo.
- In support of its crowdsource application testing service, Bugcrowd publishes the State of Bug Bounty Report 2016 – Bugcrowd report (a few key findings below):
  - Bugcrowd tracked 286 total programs, and of these, 63% were private programs and the remainder were public. Interestingly, it was not just programmers, software providers, or OS providers that offered bug bounties. Nearly one-quarter of the bounty programs were offered by companies in vertical markets (like financial services and banking).
  - Bugcrowd reports there were $2,054,721 paid out across 6,803 paid submissions.
  - The average payout per submission increased from $200.81 in the 2015 State of the Bug Bounty report, to $294.70 in the 2016 report.

Source: Frost & Sullivan analysis.

Pwn2Own

- In October 2015, Trend Micro announced plans to acquire HPE TippingPoint as well as the Digital Vaccine Labs (DVLabs), that provides real-time threat intelligence and a taxonomy to analyze vulnerabilities and exploits.
- Along with TippingPoint and DVLabs, Trend Micro also decided to keep the Zero Day Initiative which is the source of the vulnerability reporting presented in this report.
- An important technical and cultural offspring of the Zero Day Initiative is the Pwn2Own contest sponsored by then HPE and now Trend Micro ZDI.
- The first Pwn2Own contest occurred in 2007 at the CanSecWest security conference. In what amounts to a digital version of “capture the flag,” an attacker must pwn (or demonstrate control) over an application.
- Pwn2Own is the premier bug bounty contest in the world in terms of historical importance and in terms of the size of the bounties offered.
- In the history of Pwn2Own over $2.5 million in prizes have been awarded (see table on the following page).
- The Pwn2Own contest brings notoriety to research teams and to individual ethical hackers alike. VUPEN has been the most successful team, but Keen Team and MWR labs have enjoyed success as well.
- Importantly, the technical details of the “pwn” are provided to the companies that won the OS.
- In 2012-2014, a separate competition was held for mobile devices. The motivations for the Mobile Pwn2Own are the same as the Pwn2Own: to gain knowledge about the vulnerability surface of mobile devices, and to be a showcase for hackers and hacking teams (see Mobile Pwn2Own Competition).
- The 2015 Mobile Pwn2Own contest was suspended, but event organizers are planning a 2016 Mobile Pwn2Own event in Tokyo, Japan.

Source: Frost & Sullivan analysis.

Pwn2Own Competition

History of Prizes Awarded in the Pwn2Own Contest

Year	Prizes Awarded	Biggest Prize Winner (If Known)	(Discoveries/Target Types)
2007	$10,000	Dino Dai Zovi	Dai Zovi and Shane Macauley discovered vulnerabilities to Quicktime (Safari)
2008	$10,000	Charlie Miller, Jake Honoroff and Mark Daniel of Independent Security Evaluators. (Awarded on 2nd day of the contest).	Charlie Miller was able to exploit an iPhone using a security bug found in Safari.
2009	$10,000	Within minutes of the contest opening, Charlie Miller hacked into a MacBook.	The target types were mobile phones that ran BlackBerry, Android, iPhone, Symbian and Windows Mobile OS.
2010	$50,000	Based on the schedule of awards, Charlie Miller and Ralf-Philipp Weinmann/Vincenzo Iozzo won $15,000 a piece.	The available cash pool climbed to a possible $40,000 for hacks to Web browsers, and $60,000 for mobile phones.
2011	$30,000	VUPEN won $15,000 for an Apple Safari browser hack.	By the end of the contest, Apple Safari, Internet Explorer, iPhone 4, Blackberry Torch 9800 were exploited.
2012	$90,000	VUPEN was the top points corer and won $60,000.	VUPEN was able to "pwn" Internet Explorer 9, Google Chrome, and Apple Safari. Significantly, Google felt that there was a credibility gap because contestants did not need to disclose the full exploit.
2013	$480,000	VUPEN claimed $250,000	HP TippingPoint put $560,000 on the line for the first to hack Google Chrome, Internet Explorer, Java, and Adobe Flash and Reader.
2014	$850,000	VUPEN won $400,000 over two-days.	In Day One of the competition, successful attackers were launched against five products including MAC OS X, and Internet Explorer. Day Two saw successful exploits against Adobe Flash, Google Chrome, and Adobe Reader.
2015	$552,500	Jung Hoon Lee (aka lokihardt) won $225,000	Bounties were set on Google Chrome, Microsoft Internet Explorer, Firefox, Adobe Reader and Flash, Apple Safari. All targets were pwned.
2016	$460,000	Tencent Security Team Sniper (KeenLab + PC Manager) won $142,500 and was declared Master of Pwn.	The number of vulnerabilities discovered by OS at 2016 Pwn2Own were: Microsoft Windows: 6, Apple OS X: 5, Adobe Flash: 4, Apple Safari: 3, Microsoft Edge: 2, Google Chrome: 1

Source: Frost & Sullivan analysis.

Mobile Pwn2Own Competition

History of Prizes Awarded in Mobile Pwn2Own Contest

Year	Prizes Awarded	Biggest Prize Winner (If Known)	(Discoveries/Target Types)
2012	$60,000	Research teams MWR Labs, and Certified Secure each won $30,000.	In the initial Mobile Pwn2Own contest, HP offered $200, 000 in prizes. Notably, Blackberry and Cellular Baseband were not exploited.
2013	$117,500	Pinkie Pie won $50,000.	HP with sponsorship from Google Android, Chrome, and Blackberry created a pool of over $300,000 in potential prizes. Category types included physical access, Web browser, mobile app/OS, messaging service, or baseband.
2014	$350,000 est.	Four different teams claimed $75,000 for short-range wireless exploits.	The Mobile Pwn2Own contest was held in Tokyo. Nico Joly exfiltrated a Windows Phone and was able to exfiltrated cookies. Juri Aedia hacked Firefox.
2015	Not held	Nico Golde, Daniel Komaromy, Guang Gong (Qihoo 360)	Results shown are for Mobile systems exploited in the 2015 Pwn2Own contest include Samsung Galaxy 6 Baseband, and Nexus 6 Chrome.
2016	Oct 26 and 27	Contest Resumed	To be held at the PacSec Security Conference in Tokyo, Japan.

Source: Frost & Sullivan analysis.

Market Overview—The Role of MITRE and CVSS Scoring

- Since 1999, the MITRE Corporation is responsible for certification and accreditation of the Common Vulnerabilities and Exposures (CVE), enabling standardization on how public vulnerabilities are tracked, managed, and stored.
- The MITRE Corporation is a not-for-profit company that operates multiple federally funded research and development centers (FFRDCs) that provide innovative, practical solutions for some of the United States critical challenges. This corporation operates the National Cyber Security FFRDC to enhance cyber security and protect national information systems.
  - Funding for the MITRE Corporation comes from the National Cyber Security Division of the United States Department of Homeland Security.
- The MITRE documentation defines CVE identifiers (also called CVE numbers, CVE-IDs and CVEs) as unique common identifiers for publicly known information-security vulnerabilities in publically released software packages.
- In other words, the CVE is a dictionary of common names for publicly known information security vulnerabilities. CVE's common identifiers facilitate sharing of data across separate network security databases and tools and provide a baseline for evaluating the coverage of an organization's security tools, which in turn, enable a quick and accurate assessment of how to remediate vulnerabilities.

Source: Frost & Sullivan analysis.

Market Overview—The Role of MITRE and CVSS Scoring (Continued)

- CVEs (vulnerabilities) are assigned by a CVE Numbering Authority (CNA); there are three primary types of CVE number assignments:
  - The MITRE Corporation functions as editor and primary CNA.
  - Various CNAs assign CVE entries for their own products (i.e., Microsoft, HPE, Oracle, etc.).
  - Red Hat (multinational software company providing open-source software products) also provides CVE numbers for open source projects that are not a CNA.
- CVEs are used by the Security Content Automation Protocol (SCAP - finds vulnerabilities and offers methods to define those findings in order to evaluate the possible impact).
- CVEs are listed on MITRE's system as well as the U.S. National Vulnerability Database (NVD).
- NVD is the U.S. government's repository of standards-based vulnerability management data for SCAP. Utilizing SCAP this data enables automation of vulnerability management, security measurement, and compliance.
- The NVD is the CVE dictionary augmented with additional analysis, a database, and a fine-grained search engine, which makes the NVD a superset of CVE.
- The NVD is synchronized with CVE such that any updates to any CVEs (vulnerabilities) appear immediately on the NVD.
- Often a security vendor will assign a CVE score based upon either its lab findings or the vulnerability reporting of their contributors. To normalize the data in this study, *Frost & Sullivan used the final CVSS v.2 score as posted on the NVD Website as well accepting the* ***Vulnerability Type*** *as the final and definitive threat analysis data (see next page).*

Source: Frost & Sullivan analysis.

Market Overview—The Role of MITRE and CVSS Scoring (Continued)

- The NVD uses the Common Vulnerability Scoring System (CVSS) Version 2, which is an open standard for assigning vulnerability impacts and is designed to convey vulnerability severity and help in determining urgency and priority of organizations' responses.
- The NVD provides the following severity rankings per CVE-ID based on the CVSS, the system assigns a numeric value between 0 – 10, with higher scores representing greater severity:
  - Vulnerabilities are labeled "Critical to High" severity if they have a CVSS score of 7.0 - 10.0.
  - Vulnerabilities are labeled "Medium" severity if they have a CVSS score of 4.0 – 6.9.
  - Vulnerabilities are labeled "Low" severity if they have a CVSS score of 0.0 – 3.9.
  - Some vulnerabilities may not have enough information to assign a CVSS score leaving it as a "Not Applicable or NA" ranking.
- Currently, the NVD site also publishes CVSS v.3 details as well as CVSS v.2 data—a change that did happen in 2015. Later in the report, we will discuss the differences between the two metrics.
- Worth noting, while there are inherent advantages to the depth of scoring in the CVSS v.3 scoring system, many vendors have been reticent to use the new scoring. The reason is most companies that offer vulnerability assessment products use CVSS scoring as just one factor in determining the nature of a vulnerability in the context of a risk management reporting and remediation cycle.

Source: Frost & Sullivan analysis.

Research Methodology

- Vulnerability information included in this report is determined through vendor briefings, Frost & Sullivan in-house research, vendor publications, and publicly reported vulnerabilities.
- The United States Computer Emergency Readiness Team (US-CERT) Vulnerability Notes are a primary source of vulnerability data in this report.
- The National Vulnerability Database (NVD) provides severity metrics and technical data. A vulnerability must have a unique Common Vulnerabilities and Exposures (CVE) or US-CERT number assigned to qualify for inclusion as a vulnerability in this report.
- The following sentence may feel like semantics, but is important. For companies included in this study, they must have a mechanism for disclosing vulnerability data to the public. The companies included here have a Web page devoted to vulnerability disclosure information.
- At a minimum, the disclosure of a threat must have a CVE number and public disclosure date.
- Frost & Sullivan requires CVE numbers for report inclusion to eliminate the double reporting of vulnerabilities. This ensures that each vulnerability report counted represents a single vulnerability.
- The NVD provided Common Vulnerability Scoring System Version 2.0 (CVSS V2) scores and rankings for each vulnerability reported. (Note: CVSS V3 is being phased in).

Source: Frost & Sullivan analysis.

Research Methodology (continued)

- CVSS is a widely accepted industry standard and is applied to most reported vulnerabilities.
- CVSS provides a base score that represents the innate characteristics of each vulnerability. This base score does not account for temporal and environmental conditions.
- In addition to the numeric CVSS scores, this report provides a severity ranking for each vulnerability mapping qualitative rankings to numeric CVSS scores.
- This report also includes original vulnerability discoveries that are reported on research vendor Websites. For a complete list of sources referred to in this report see List of Publications Cited in This Report.
- The formal reporting focuses on the base year 2015. In many cases, direct comparisons are made with the 2014 publicly reported vulnerabilities.

Source: Frost & Sullivan analysis.

Types of Threats

Malware

- The majority of this report is focused on software vulnerabilities that are publicly disclosed and given Common Vulnerability Scoring System (CVSS) v.2 scores.
- However, a small but important point to realize is that the vast majority of vulnerabilities are never acted upon (i.e., exploited). In an IBM study, IBM found that 80% of all vulnerabilities were not acted upon. Ostensibly, there would be a correlation between a largely vulnerable endpoint or application and the occurrence of a formal exploit.
- It is possible that devices/servers/applications with a low vulnerability score like “1” or “2” can be exploited, while other endpoints/applications with a “10” score are left unscathed (probably not for long if there is a public disclosure).
- While the emphasis of this report is on public disclosure and vulnerable software, it seems relevant to review the types of outcomes that infect the business and security landscape.
- This is a simple but declarative statement, “Binaries that perform decidedly ‘bad’ actions are considered malware.”
- Ideally, malware is deflected at the perimeter defense (typically an antivirus defense system or denied access from a firewall). Additionally, common sense precaution such as the physical security of devices, and software written without bugs or vulnerabilities within the source code, help to add to an optimal security posture.
- Rarely are security practice perfectly implemented in the real world. Besides that, hackers continue to create new ways to attack and exploit.

Source: Frost & Sullivan analysis.

Malware (continued)

- Hackers also are finding ways to glean information from social media Websites.
- Two developments—Heterogeneous networking and the Internet of Things— are adding depth to communications platforms. Unfortunately, the same new networking systems that create agility for businesses are also ways for hackers to access networking systems.
- Smartphones, tablets, and purpose-built (proprietary) devices that use the Internet for personal and commercial applications. Mobile represents a new frontier for apps developers and would-be attackers alike.
- Many of the companies that Frost & Sullivan is working with in the development of this report are producing excellent content in the context of all types of vulnerabilities.
- Symantec deploys over 63 million attack sensors globally and charts activities from 157 companies. At the end of 2015, some larger headline threat data information published by Symantec includes:
  - An increase in zero-day vulnerabilities discovered by Symantec from to 54 in 2015, from 23 in 2014.
  - Crypto ransom attacks increased from 269,000 events to 362,000 attacks in 2015 are becoming more pervasive in 2016.
  - If there was a breach that unclosed “identities,” the average number of identities exposed in the breach rose to 1.3 million in 2015—the number of which were ever exploited for profit is both unknown and possibly disruptive.

Source: Frost & Sullivan analysis.

Malware (continued)

- Cisco Labs collects vulnerability, exploit, and advanced persistent threat (APT) from multiple network security appliances and platforms including Cisco's network security platforms including next generation firewalls, intrusion protection systems (IPS), Web and Email content security, network access control (NAC), and Cisco Cloud and Managed Service Program (CMSP).
- The Cisco 2016 Annual Security Report proffered these facts about malware:
  - Cisco found 91.3% of malware used a Domain Name Service (DNS) to carry out attacks.
  - Cisco found there were roughly 15,000 sites that pushed the Angler exploit kit and about 60% of these delivery systems included a ransomware variant.
  - Cisco offers the OpenDNS malware defense technology and discovered that 68% of organizations do not offer recursive DNS monitoring.
  - Cisco surveyed its own Cisco Custom Threat Intelligence. Cisco detected evidence of the Angler Exploit Kit, Cutwall Spam Botnet, and Drye had infected 4 out of 5 networks environments.

- Like Cisco, Hewlett Packard Enterprise (HPE) produces an annual security report. Its is titled the HPE Security Research Cyber Risk Report 2016. HPE offers these insights;
  - In partnership with ReversingLabs, HPE found that the Allaple polymorphic worm was the malware variant most likely used to attack a Windows system with 26% of attempted attacks. Elkern, which acts like a parasite, was deployed in 19% of Windows attacks.
  - In attacks on OS X systems, the Macnist was the most potential unwanted application installed with it being the source of 62% of malware launched from application in OS X environment. The VSearch plug-in became a threat vector in 30% of attacks emanating from applications in OS X environment in 2015.
  - The top type of attack that launched against Linux were distributed denial of service (DDoS) attacks.

Source: Frost & Sullivan analysis.

Malware (continued)

- The most fascinating thing about malware is not its existence, malware and cockroaches will survive the global apocalypse, rather, it is the evolving philosophies about what constitutes a successful network security posture.
- Serious network security practitioners will advocate a layered approach. Secondly, the concept of friction becomes important. While a sophisticated attacker may have patience and tactics designed to defeat a layered attack, it is important to offer as much resistance as possible to would-be hackers.
- In some schools of thought, perimeter defenses have been viewed as *de classe*. However, with the use of API creating bidirectional communication from knowledge-based security tools that reside on switches and SPAN ports, both interior and exterior defenses can be dynamically improved with shared knowledge.
- Even as this occurs, additional threat intelligence knowledge can be gained by using behavioral analytics or correlating log and Netflow data against statistical baselines.
- Lastly, the idea of friction becomes important. While the skills base of hackers is improving, it is absolutely necessary to prevent hackers from stealing or altering low hanging fruit.
- Many enterprises have built in either sandbox technologies to quarantine suspicious IP traffic, or use deception to let invading bots spin benignly in what amount to a phony network.
- Of course, the saying is that the.. “best plan of mice and men,” Security practitioners remain limited by finite security budgets and limited manpower.
- In some ways, public vulnerability disclosure creates an information repository that security practitioners can leverage and implement for free.

Source: Frost & Sullivan analysis.

Mobile Malware

- Like the proliferation of mobile devices, mobile malware follows suit. According to McAfee Labs, the second quarter of 2016 had the highest ever recorded number of new mobile malware, and represented a 151% over the previous year.
- The threat of mobile malware is not limited to sheer numbers, but how cybercriminals are exploiting users and software vulnerabilities. Case in point, IBM noted in this article that:

One of the key contributors to the threat from mobile malware is the proliferation of applications that conduct real business using access-sensitive and confidential information. Typical users may have banking, credit card, hotel, airline and corporate applications installed on their mobile devices. This access is secured, at minimum, with username and password controls.

And added this staggering observation on mobile applications:

Take a look at the version history of some of the most popular mobile apps. Many released 10 or more updates last year — and that's on a single mobile platform! The continuous release cycle puts pressure on developers, who in turn may make mistakes in their haste.

- There are steps that organizations can take to lower their mobile malware risk, such as, designate sources of mobile applications (i.e., trusted sources). Nevertheless, the business dependency on mobile applications and the rate of application updates will almost guarantee exploitable vulnerabilities.

Source: Frost & Sullivan analysis.

Mobile Malware (continued)

- In practical terms, these vulnerabilities are not limited to mobile operating systems and applications, but extend to the software vulnerabilities resident on corporate laptops, servers, and non-mobile commercial applications.
- The reason is simple, the mobile device is not just a device to infect and exploit, but a doorway to corporate systems where a larger pool of digital assets are present for hackers to pilfer. Therefore, remediating software vulnerabilities must be “on all devices” in order to maximize effectiveness.

Source: Frost & Sullivan analysis.

Ransomware

- Ransomware, as a malware category, is growing in size and impact
- From a growth perspective, McAfee Labs has documented a continuous increase in ransomware samples. In its latest reporting period, the second quarter of 2016, new ransomware samples totaled over 1.3 million. On an annual basis, ransomware samples increased 128% and exceeded 7 million.
- Regarding impact, Malwarebytes reports from a survey it sponsored in 2016, 39% of businesses experienced a ransomware attack in the last year, and 37% of them paid the ransom. As we described in *War on Ransomware - No Silver Bullet Defense, but Indifference is Not an Option Either*, the cost of ransomware is not limited to the ransom. Other "costs" include: lost productivity, reduced revenue, brand damage, and remediation effort.
- Contributing to this growth in ransomware's size and impact are the following:
  - Systematic and scalable malware development is common
  - Tried-and-true malware delivery mechanisms continue to be effective (e.g., phishing emails and drive-by Website downloads)
  - A broader footprint exists as businesses, not just consumers are targeted
- While there are several defenses that businesses can employ to reduce their ransomware risk (circumvent ransomware distribution, contain the infection, declaw lateral movement), standard security hygiene should be practiced, including removal of known vulnerabilities as they can be enablers of ransomware's effectiveness as noted in this Dark Reading article: CVE-2015-7645, CVE-2015-8446, CVE-2015-8651, and CVE-2016-0034.

Source: Frost & Sullivan analysis.

Bots and Botnets

- Bots (short for “robots”) is the term used for any program that executes a simple set of instructions on the Web in an automated manner. Bots typically feature simple programming to perform an action or series of actions repeatedly as directed by the bot owner.
- As a result, bots come in a range of varieties based on what actions they perform, from Web indexers, and Web scrapers, to scalpers, DDoSers, and spammers. Yet the term “bots” has a negative connotation that focuses on malicious bots such as DDoSers, spammers, and credential testers.
- Bots are most effective when combined in a large coordinated network called a botnet. The collective efforts of a botnet can be used to harass even the largest online organizations.
- Understandably, businesses are very interested in solutions that can stop the “obvious malicious” bots from interacting with Web assets.
- However, many bots fall into a moral grey area. Bots that are designed to collect data from competitor Websites might not be breaking any laws but places the data owners at a competitive disadvantage.
  - A well documented example of this is in the travel and hospitality industry. Travel agencies and airlines post their fares online to aid customers with their travel plans. Unfortunately, competitors can see this data as well, and use bots to collect valuable data such as pricing data, then price match or undercut the competitors’ fares.
- Simply blocking all bots is not an option either. Many organizations use bots to communicate with partners and rely on Web crawlers to appear at the top of search engine results.

Source: Frost & Sullivan analysis.

Bots and Botnets (continued)

- As a result, businesses require solutions that do not offer over simplified “good bot” or “bad bot” assessment or blunt “block or allow” controls. For example:
  - Desirable bots may need to be allowed but may also need to be slowed down.
  - Bad bots may need to be blocked; however, other options such as “slow down” or “feed alternate data” may be more useful.
  - A myriad of bots fall into grey areas and may require a range of actions from “nothing at all” to “redirect,” or “slow down.”
- Many businesses are beginning to grasp the complexity of the bot problem. As a result, demand for complete bot management solutions is expected to grow at a high rate in coming years.
- Akamai and Imperva are two companies that are now offering completed, dedicated bot management while emerging companies such as PerimeterX and Shape Security are focused on advanced bot mitigation solutions.
- For additional information about bots and botnets, see Bots to the Future: The Emerging Market for Bot Management Solutions.

Source: Frost & Sullivan analysis.

Advanced Persistent Threats (APT)

- The term “advanced persistent threat” (APT) came into prominence to reference the emerging class of malware and tactics used in some of the most high profile data breaches such as Stuxnet, Flame, Gauss, and Operation Aurora. Many of these threats were discovered between 2010 and 2012 but were found to be operating for years.
- APTs have a number of attributes that separate them from traditional cyber threats:
  - APTs are sophisticated and use advanced techniques to evade detection, cover evidence of their activities, and enact subtle but damaging attacks.
  - APTs are targeted to specific high value organizations. Attack techniques are tailored to exploit specific weaknesses in the target organization’s defenses. Often, threat actors save their most advanced techniques and zero-day vulnerabilities for use against high value targets.
  - APTs are persistent. The malware utilized may be resilient and survive traditional remediation efforts and once detected, attackers will simply try to find alternative inroads.
- These attributes made APTs difficult to stop with conventional network security tools.
- The effects of an APT breach can be catastrophic. Stuxnet was designed to sabotage industrial facilities, Operation Aurora sabotaged the intellectual property of some of the largest software companies in the world. Today, enterprises continue to be harassed by ransomware and other destructive advanced malware and APTs.
- As a result, the need to stop APTs is urgent.

Source: Frost & Sullivan analysis.

Advanced Persistent Threats (APT) (continued)

- Today, APT defense requires a coordinated set of processes and security tools.
- Advanced malware sandbox (AMS) analysis is a popular tool for combating APTs.
  - AMS operates by identifying suspicious files, extracting them, and executing them in a virtual environment that simulates a target endpoint system. The actions of the suspected file are then observed and any malicious behaviors are noted.
  - Binaries that are found to be malware are blocked (dropped from network traffic) and any necessary investigation and remediation steps are initiated.
  - According to Frost & Sullivan research the market reached nearly a billion dollars in 2015. See Advanced Malware Sandbox Market Analysis, September 2016.
- Other means of APT defense involve monitoring the network environment and endpoints for indicators of compromise (IOCs). Correlation of multiple otherwise independent signals can help to find a data breach perpetuated by an APT.
  - This may be accomplished by SIEM solutions or other network monitoring tools.

Source: Frost & Sullivan analysis.

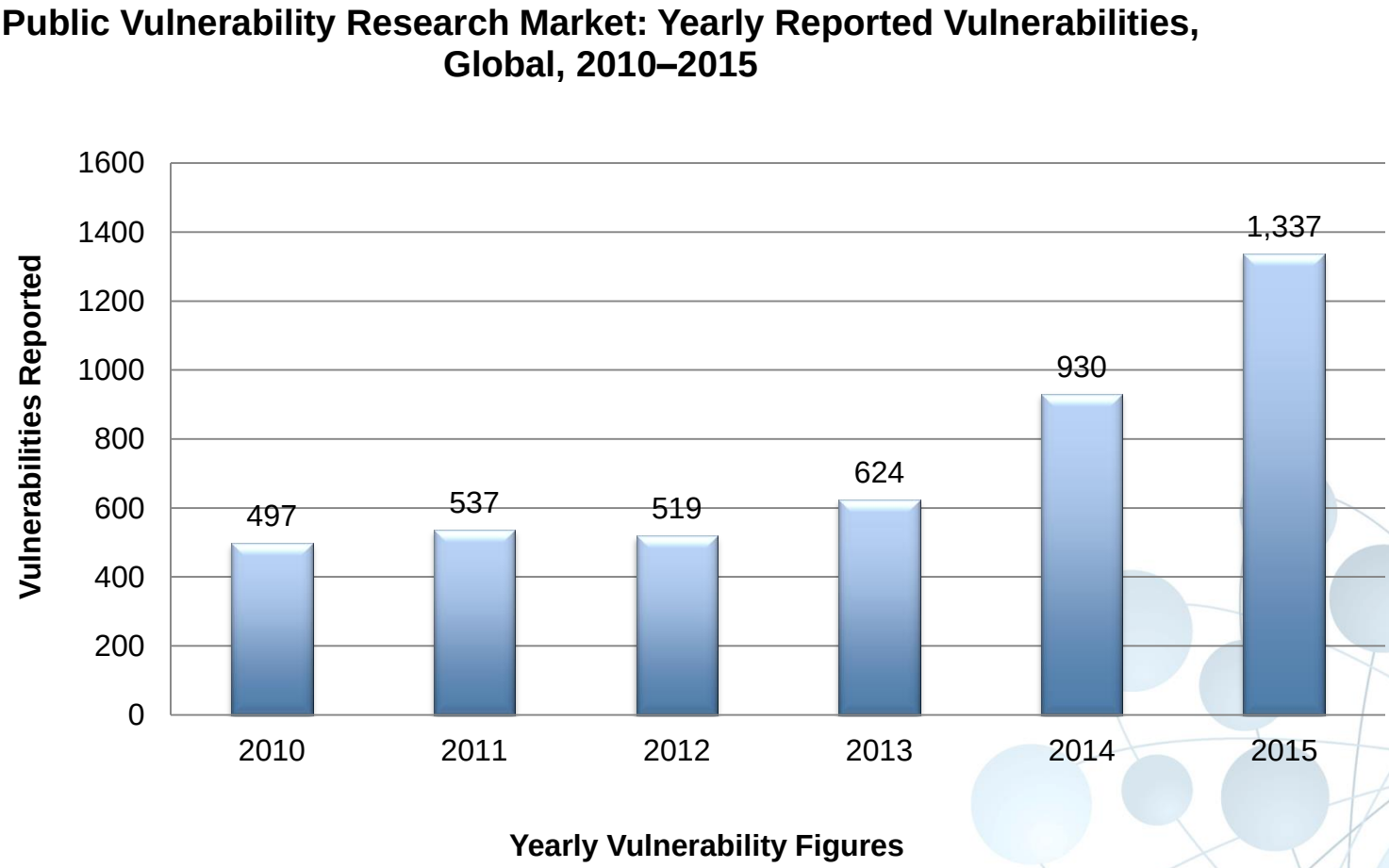
Web and Phishing Attacks

- For the past few years most of the participating public vulnerability research firms made the observation that vulnerabilities have been migrating toward the Web and toward Web-based applications. While threats detected toward Web applications were slightly down as an overall percentage, as Frost & Sullivan found 207 vulnerabilities (or 15.5% of all vulnerabilities) directly related to Web applications.
- In 2015, Symantec found 431 million malware families; up from the 317 million malware families found in 2014.
- Of course, the best form of threat mitigation is to block the miscreant from arriving in the first place. In 2015, Symantec reports that it was able to block over 100 million fake technical support scams.
- In the often dark haunts of cyber security threat reporting, one ray of light comes through. Symantec reports that the email phishing rate is regressing.
- In 2013, 1 in 392 emails were designed for phishing attacks. In 2014, that rate changed to 1 in 965, and in 2015, that was 1 in 1,846. (Note, Symantec excluded spear phishing in this analysis).
- In refining its research for 2015, Secunia cataloged vulnerabilities relating to the five most popular browsers (Google Chrome, Mozilla Firefox, Internet Explorer, Opera and Safari3). The change in vulnerabilities found was slight moving from 1,076 vulnerabilities in 2014 to 1,114 vulnerabilities found on these browsers in 2015: an uptick of 4%.
- One useful piece of information from that study is the use of multiple browsers on PCs is the norm and not the exception. Internet Explorer has a 99% market share followed by Chrome (66%) and Firefox (64%).

Source: Frost & Sullivan analysis.

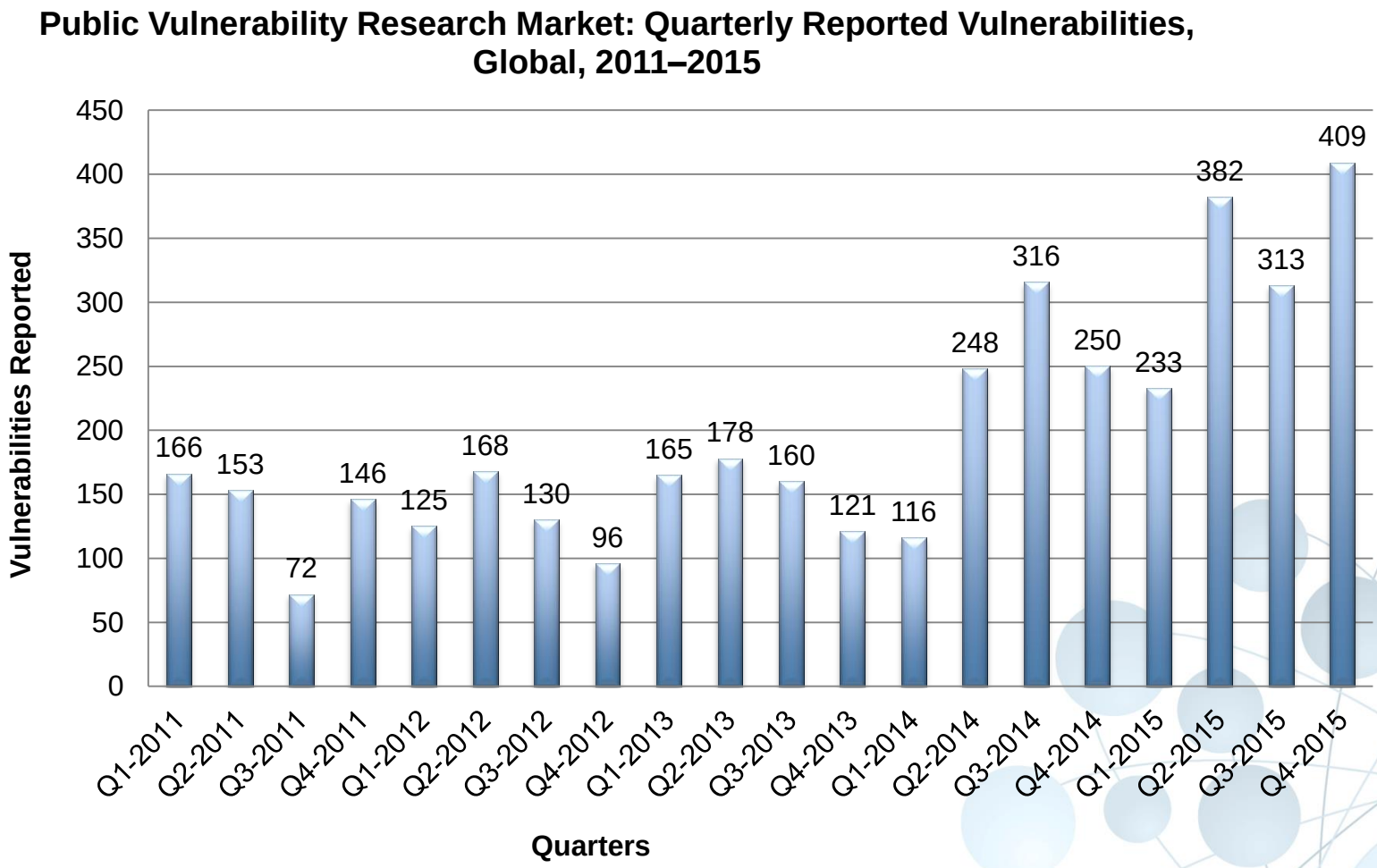
Market Trends in Public Vulnerabilities

Vulnerabilities Reported by Year



Note: All figures are rounded. The base year is 2015 Source: Frost & Sullivan analysis.

Quarterly Reported Vulnerabilities



Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Market Trends

- From January 1, 2015 through December 31, 2015, there were 6,422 vulnerabilities assigned Common Vulnerabilities and Exposures (CVE) numbers.
- Many of these numbers were reserved in good faith. However, in certain cases, MITRE will not be able to confirm the vulnerability and the CVE number is held in reservation. However, roughly 85 percent of the vulnerabilities given a CVE number will be verified and given a CVSS score.
- Frost & Sullivan recounts 1,337 publicly reported and verified vulnerabilities. Frost & Sullivan only includes the vulnerabilities for which the NVD issued a public disclosure. Publicly disclosed implies that the vendor and the disclosing agency make a joint statement.
- Trend Micro ZDI had the most verified vulnerabilities reported with 656 proving the veracity of the Trend Micro contributor program. In early 2016 Trend Micro acquired the HPE TippingPoint program. All prior references to HPE TippingPoint are noted as Trend Micro ZDI.
- Cyber-attacks are largely automated; the vast majority (roughly 80%) of vulnerabilities will not be acted upon.
- IBM noted that the explosion in terms of the physical number of vulnerabilities happened between 2004 and 2006.

Source: Frost & Sullivan analysis.

Market Trends (continued)

- PAST: Customer demand drove vulnerability testing, but this factor has changed in recent years.
- PRESENT: Vulnerability testing is not an elective; companies must be able to mitigate persistent threat environments. Compliance testing is becoming more requisite as The Affordable Care Act gains traction, Payment Card Industry (PCI) Data Security Standard (DSS) 3.0 takes hold, and international markets adopt cyber defense practices. One example, the Basic Standard for Enterprise Internal Control is mandated by the Chinese government (known as C-SOX, the Chinese equivalent of Sarbanes-Oxley in the US).
- TRENDING: The Federal Government is observing NIST 800.53A, Rev.4. This standard establishes precedence for continuous monitoring.
- The Top 20 Critical Security Controls (CSC) are vendor best practices designed to reduced the attack surface.
- The Top Five CSC measures include: 1) Inventory of Authorized and Unauthorized Devices, 2) Inventory of Authorized and Unauthorized Software, 3) Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, 4) Continuous Vulnerability Assessment and Remediation, and 5) Malware Defenses.

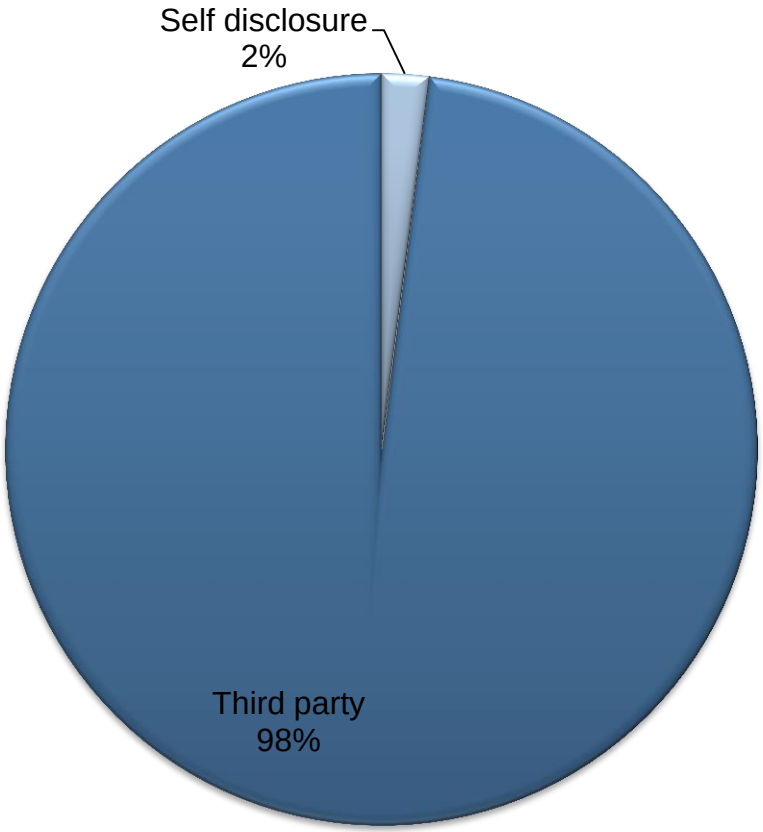
Source: Frost & Sullivan analysis.

Market Trends (continued)

- Google Project Zero was launched in mid-2014. The results have been added to the data published in a prior report.
- The addition of Google Project Zero and increasing research by Trend Micro ZDI has driven the increase in the number of confirmed vulnerabilities in 2015.
- The total number of confirmed vulnerabilities in 2015 were 1,337. This is an increase of 43.8% over the 930 in 2014.
- Trend Micro ZDI was the leading disclosing institution with 656 vulnerabilities in 2015, holding 49.1% share. This is a growth of 90.7% over 2014 and an increase in share of 12 basis points.
- Google Project Zero doubled its vulnerabilities in 2015 reaching 302. It has a share of 22.6% of total vulnerabilities, an increase of 6.4 basis points.
- The third largest disclosing institution, US-CERT, declined 15.1% in 2015 falling to 219 vulnerabilities. It holds 16.4% share of total vulnerabilities.
- On a quarterly basis there is a general upward trend. Increasing activity by researchers is resulting in the discovery of more vulnerabilities.

Vulnerability Disclosure

Public Vulnerability Research Market: Percentage of Reported Vulnerabilities by Disclosure Type Global, 2015



N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015 Source: Frost & Sullivan analysis.

Vulnerability Disclosure (continued)

- Self-disclosed vulnerabilities are vulnerabilities reported by the manufacturer of the application with the vulnerability. Third-party sources are research laboratories or individuals who report vulnerabilities in an application.
- Third-party sources continue to report the majority of vulnerabilities in 2015. Third-party sources discovered and reported 98.0% of vulnerabilities in 2015.
- Self-disclosed reports accounted for 2.0% of reported vulnerabilities.
- Manufacturers have different mechanisms for reporting vulnerabilities. Most companies issue advisories. Manufacturers like Microsoft and Oracle have a regular schedule for the release of advisories.
- Security patches are the primary method of fixing security vulnerabilities in software. A patch is a piece of software designed to update a computer program or its supporting data, to fix or improve it. This includes security vulnerabilities and other bugs improving the usability and performance.
- Whether the exploit code or the vulnerability related to the patch was never made public is a matter of semantics; a vulnerability exists.
- For PSIRTs, testing for vulnerabilities includes internal and external sources. Manufacturers continue to contract out vulnerability testing to research laboratories. The need to test Web portals and applications is now as important as testing network endpoints and configurations.

Source: Frost & Sullivan analysis.

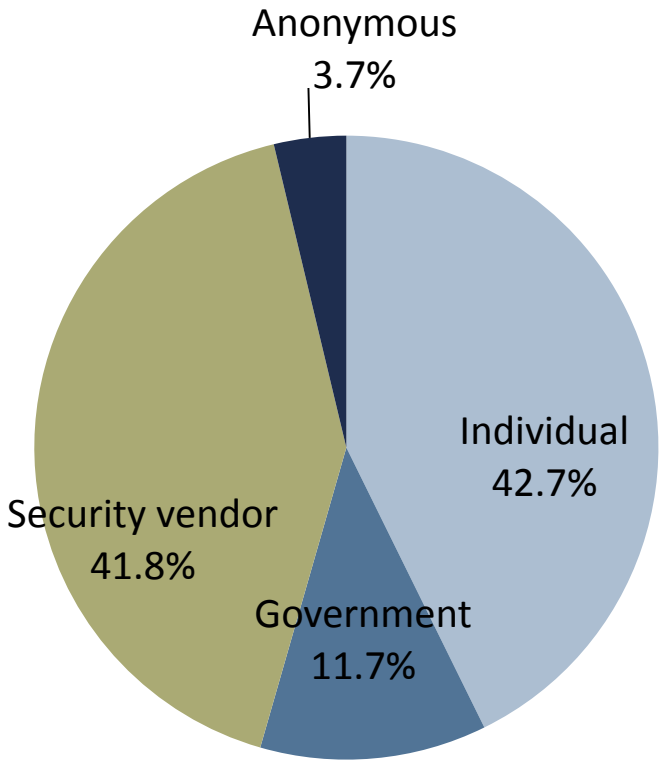
Vulnerability Disclosure (continued)

- Vulnerability disclosure is a double-edged sword. If a manufacturer discloses a vulnerability, there is an admission of a procedural weakness in the production phase.
- However, almost any application or network, at some point, will display a vulnerability. Therefore, vulnerability disclosure is part of the on-going obligation that a manufacturer has to the customer to ensure integrity.
- When working with manufacturers, security vendors may decide not to disclose some vulnerabilities because these vulnerabilities are unfixable or too expensive and resource-intensive to fix.

Source: Frost & Sullivan analysis.

Vulnerability Disclosure by Institution Type

Public Vulnerability Research Market: Percentage of Vulnerabilities by Institution Type, Global 2015

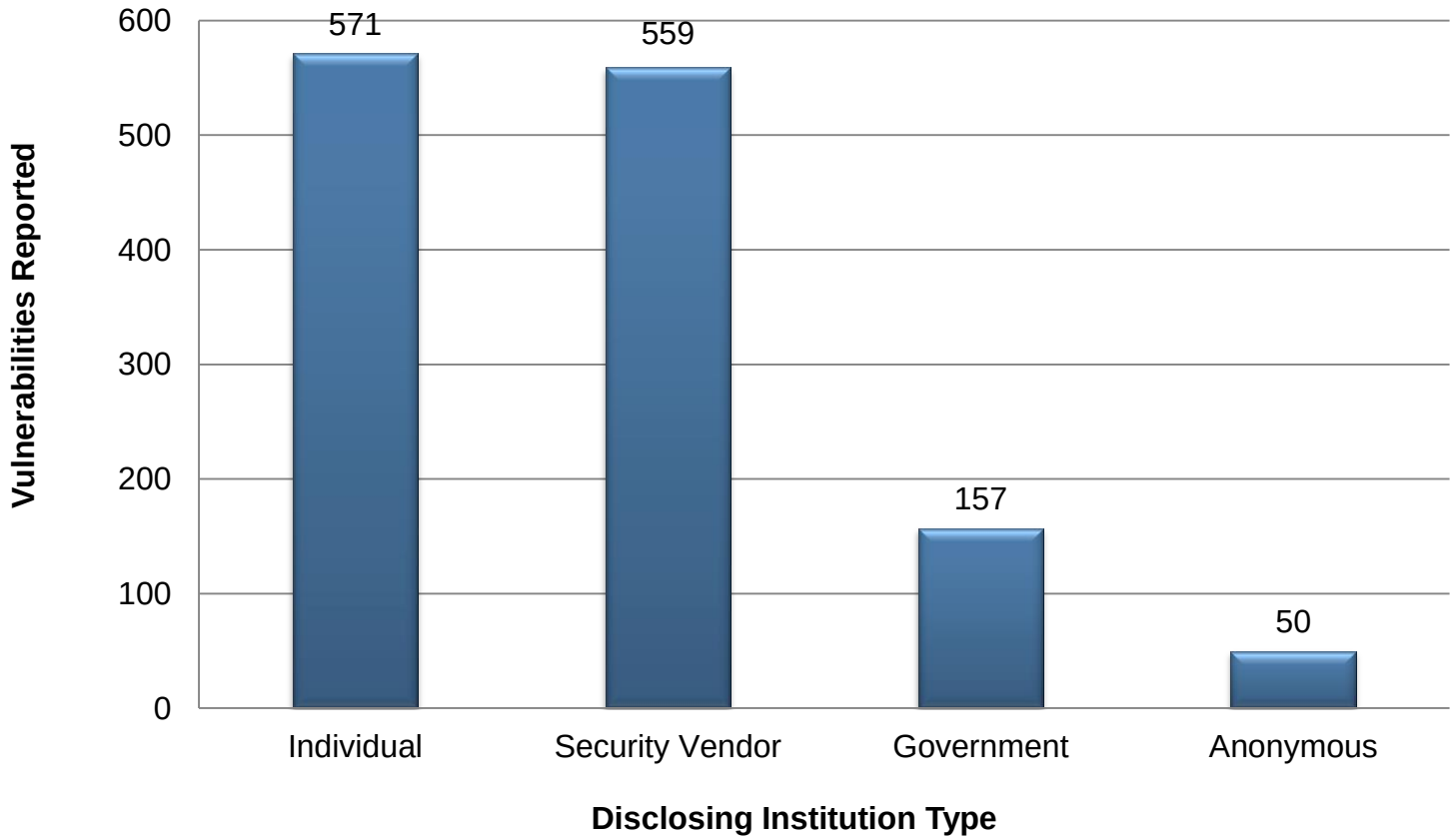


N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015 Source: Frost & Sullivan analysis.

Vulnerability Disclosure by Institution Type (continued)

Public Vulnerability Research Market: Reported Vulnerabilities by Organization Type Global, 2015



N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Vulnerability Disclosure by Organization Type (continued)

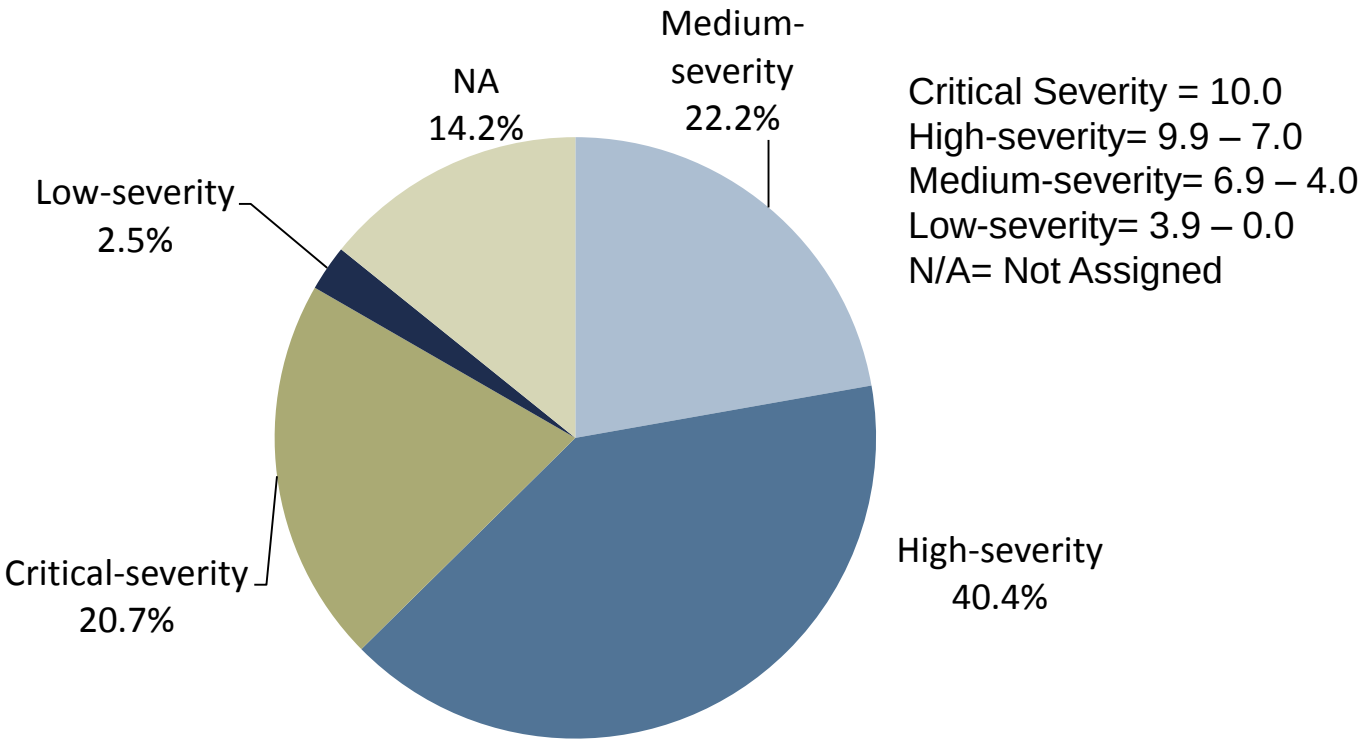
- Vulnerabilities disclosed by Trend Micro ZDI and Secunia were counted as individual if indicated in their disclosures. If the vulnerability was disclosed as Secunia Research, HPE or Trend Micro ZDI it was counted in the Security vendor category.
- Google Project Zero began in mid-2014. If a vulnerability impacts a Google product, such as Android, it is counted as a self disclosure, otherwise it is a Security vendor category.
- US-CERT vulnerabilities were counted with the Government category even if individually reported. This represented 11.7% of vulnerabilities in 2015.
- In 2015 individual attribution of vulnerability discovery was 42.7%.
- The security vendors found 41.8% of all publicly disclosed vulnerabilities.
- Fifty vulnerabilities (3.7%) were anonymously disclosed or the attribution is unknown.
- Compared to 2014, the percentage of individual contributors remained essentially unchanged, 42.0% in 2014. However, security vendor percentage increased from 29.7% in 2014. This may be attributed in part to Google Project Zero, but security vendors also work with other disclosing institutions, such as Trend Micro ZDI.
- The government segment, in particular US-CERT, dropped from 25.5% share in 2014.

Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity

Analysis of Vulnerabilities by Severity

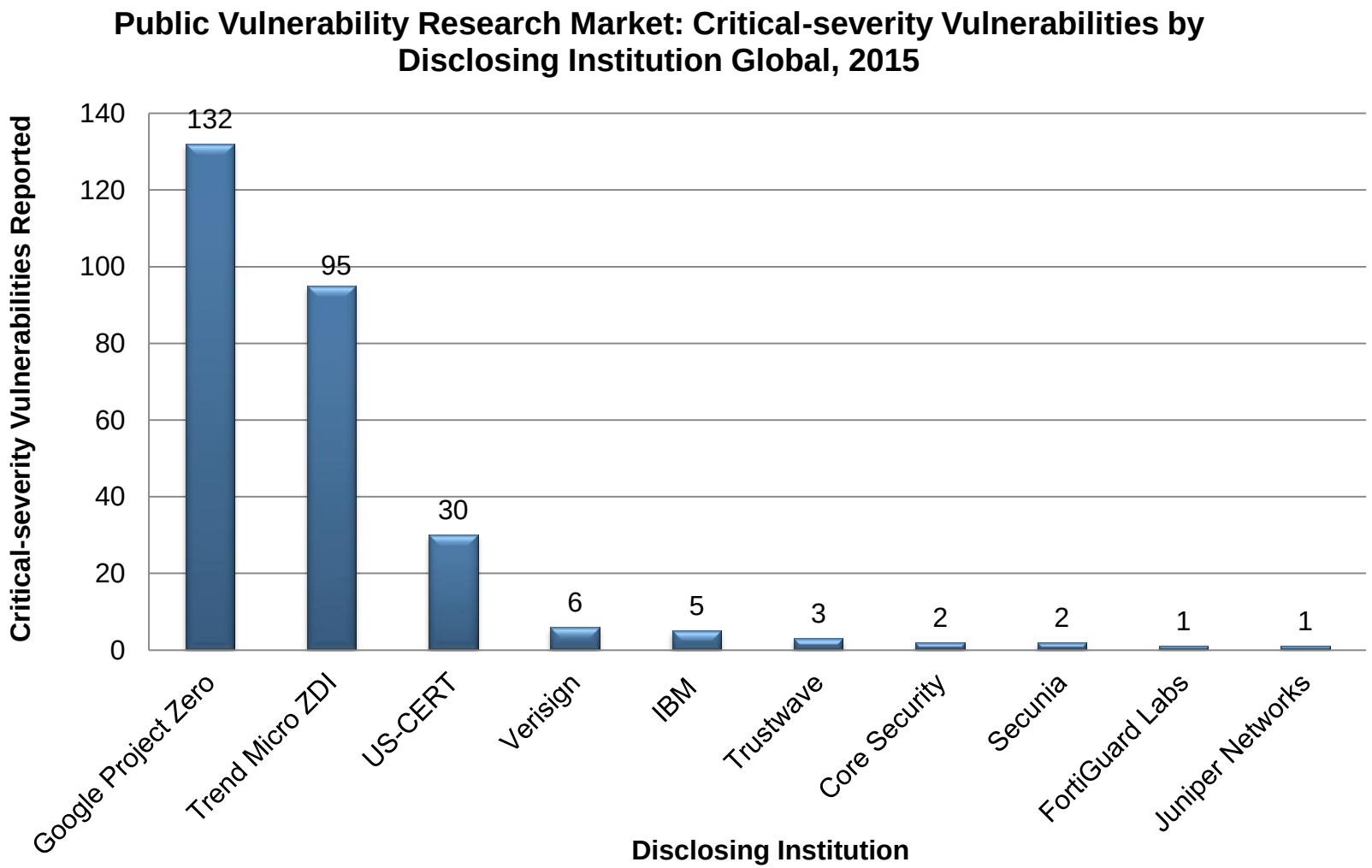
Public Vulnerability Research Market: Percentage of Reported Vulnerabilities by Severity, Global 2015



N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis

Analysis of Vulnerabilities by Severity (continued)



N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

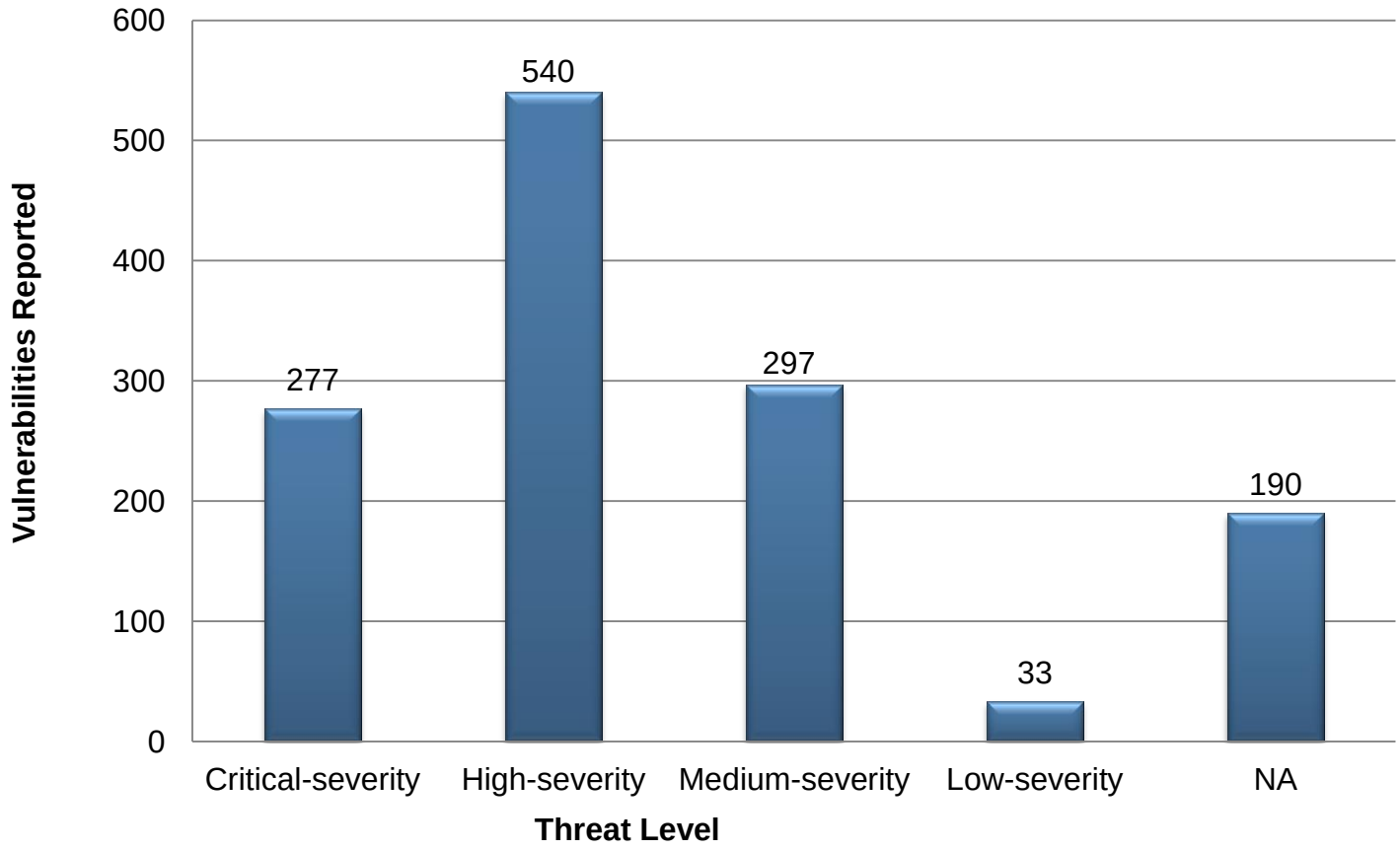
Analysis of Vulnerabilities by Severity (continued)

- The National Vulnerability Database assigned a CVSS risk rating to each vulnerability that is useful in assessing an organization's risk and remediation priorities.
- In 2015, critical vulnerabilities rated 10.0 by the NVD amounted to 20.7% of vulnerabilities disclosed. This was grew from the 16.3% share by the same disclosing institutions in 2014. In absolute numbers, 2015 increases 82.2% year over year. An increase of 4.4 basis points.
- Critical-severity vulnerabilities are potentially subject to code executions, unauthorized disclosure of information and denial-of-service attacks which can hamper or shut down an organization's operations.
- High-severity vulnerabilities accounted for 40.4% of disclosed vulnerabilities in 2015. This is up from 30.9% in 2014, an increase of 9.5 basis points. These vulnerabilities are also at risk of denial-of-service attacks and file modifications in a network's infrastructure.
- Medium- and low-severity vulnerabilities represented 22.2% and 2.5% of vulnerabilities disclosed, respectively. Medium-severity vulnerabilities declined not only as a percentage but in absolute numbers as well. Low-severity vulnerabilities were essentially flat as a percentage.
- Vulnerabilities which were unknown or not assigned a severity ranking, NA, increased dramatically from 2.6% share in 2014 to 14.2% in 2015.
- Both the total number of public vulnerabilities and percent of vulnerabilities in the critical and high risk rating categories increased year-over-year, a clear indicator that inattentiveness in remediating vulnerabilities or compensating for vulnerabilities leads to higher levels of riskiness.

Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

Public Vulnerability Research Market: Reported Vulnerabilities by Severity, Global, 2015

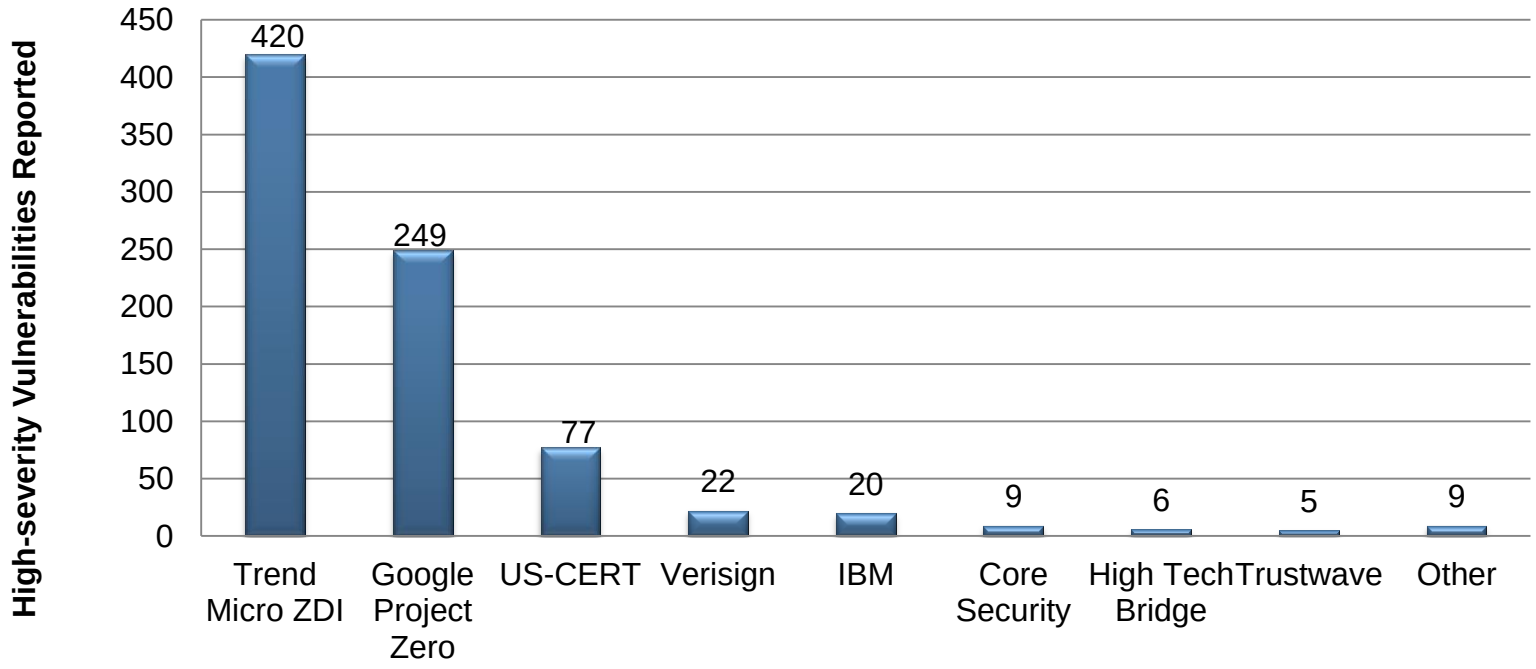


N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2016. Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

Public Vulnerability Research Market: Critical & High-severity Vulnerabilities by Reporting Source, Global, 2015



N=817 vulnerabilities

Organization

Note: All figures are rounded. The base year is 2015 Source: Frost & Sullivan analysis.

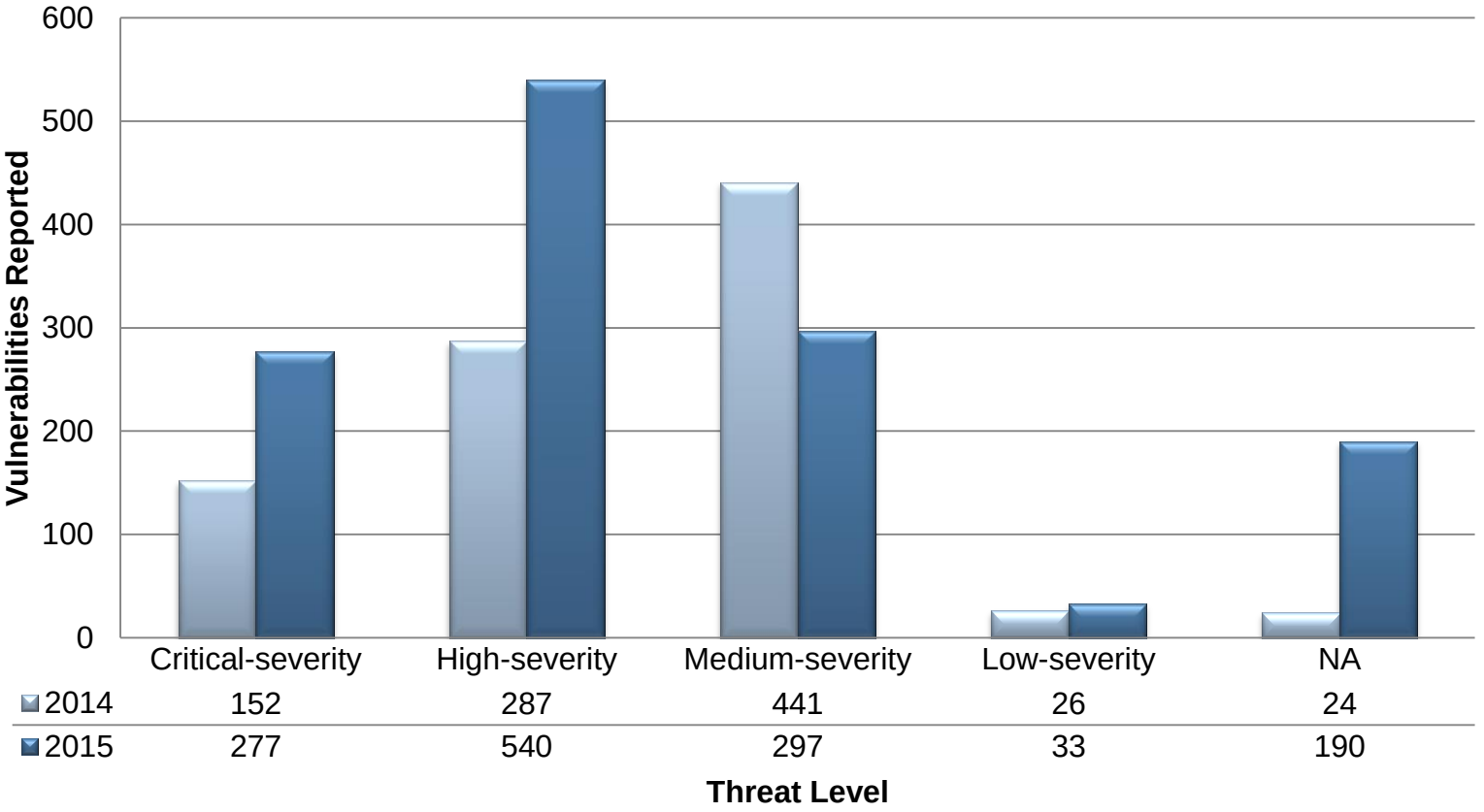
Analysis of Vulnerabilities by Severity (continued)

- The total number of vulnerabilities with a critical ranking (CVSS score = 10.0) increased 82.2% from 2014 reaching 277 in 2015.
- Google was the leading disclosing institution in reporting critical severity in 2015 with 132. This is an increase of 120.0% over 2014 and 47.7% share in 2015.
- Trend Micro ZDI is a close second in critical severity reporting 95 vulnerabilities in 2015. This is an increase of 111.1% over 2014 and 34.3% share in 2015.
- Combining Critical and High (CVSS = 9.9 to 7.0) severity rankings, the number of vulnerabilities was 817 in 2015, an increase of 86.1% over 2015. And, this percentage increase is almost double the percentage increase in total vulnerabilities.
- Trend Micro ZDI was the leading disclosing institution for Critical and High severity vulnerabilities with 420 in 2015, a growth of 160.9% over 2014. This represents 51.4% share of this segment. Trend Micro ZDI was the leader in 2014, as well. It added 14.7 basis points in 2015.
- Google was second in reporting Critical and High severity vulnerabilities with 249 in 2015. This is a 128.4% growth over 2014. Google holds 30.5% share of this segment, and increase of 5.6 basis points in 2015.

Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

Public Vulnerability Research Market: Reported Vulnerabilities by Severity, Global, 2014 and 2015

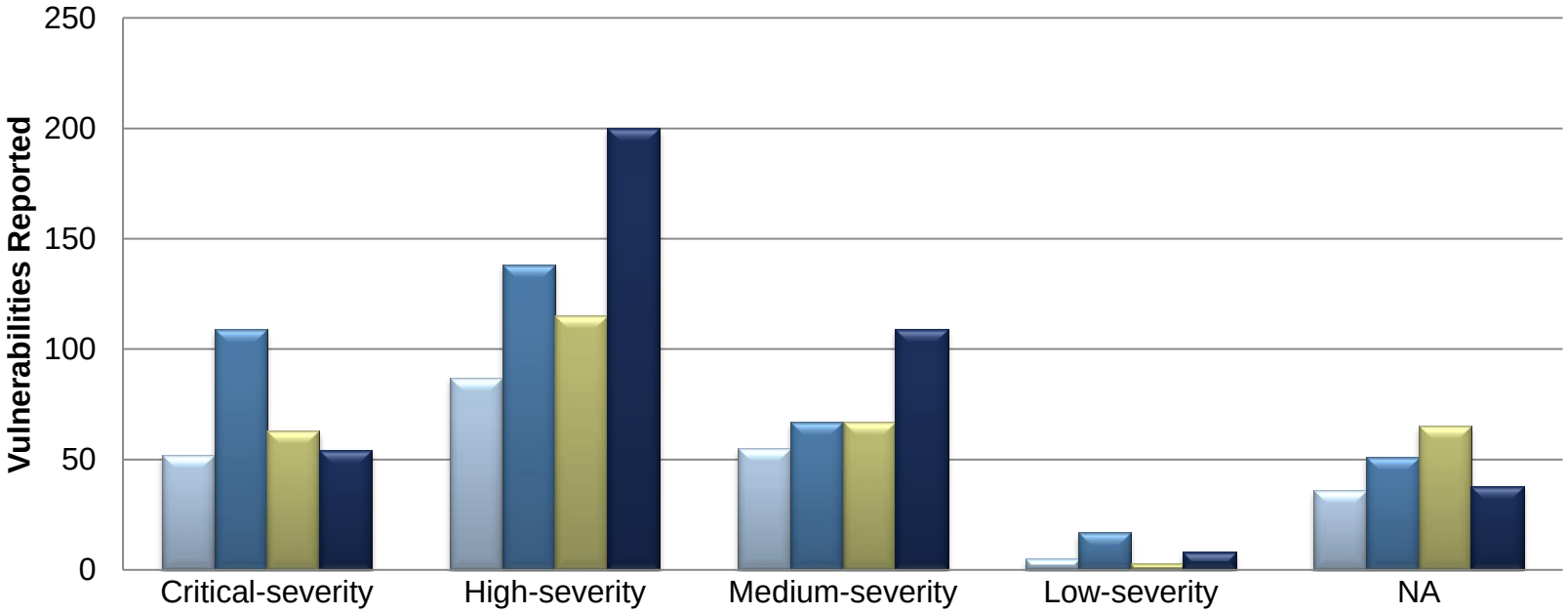


N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015 Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

Public Vulnerability Research Market: Reported Vulnerabilities by Quarter and Severity, Global, 2015



	Critical-severity	High-severity	Medium-severity	Low-severity	NA
Q1	52	87	55	5	36
Q2	109	138	67	17	51
Q3	63	115	67	3	65
Q4	54	200	109	8	38

N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

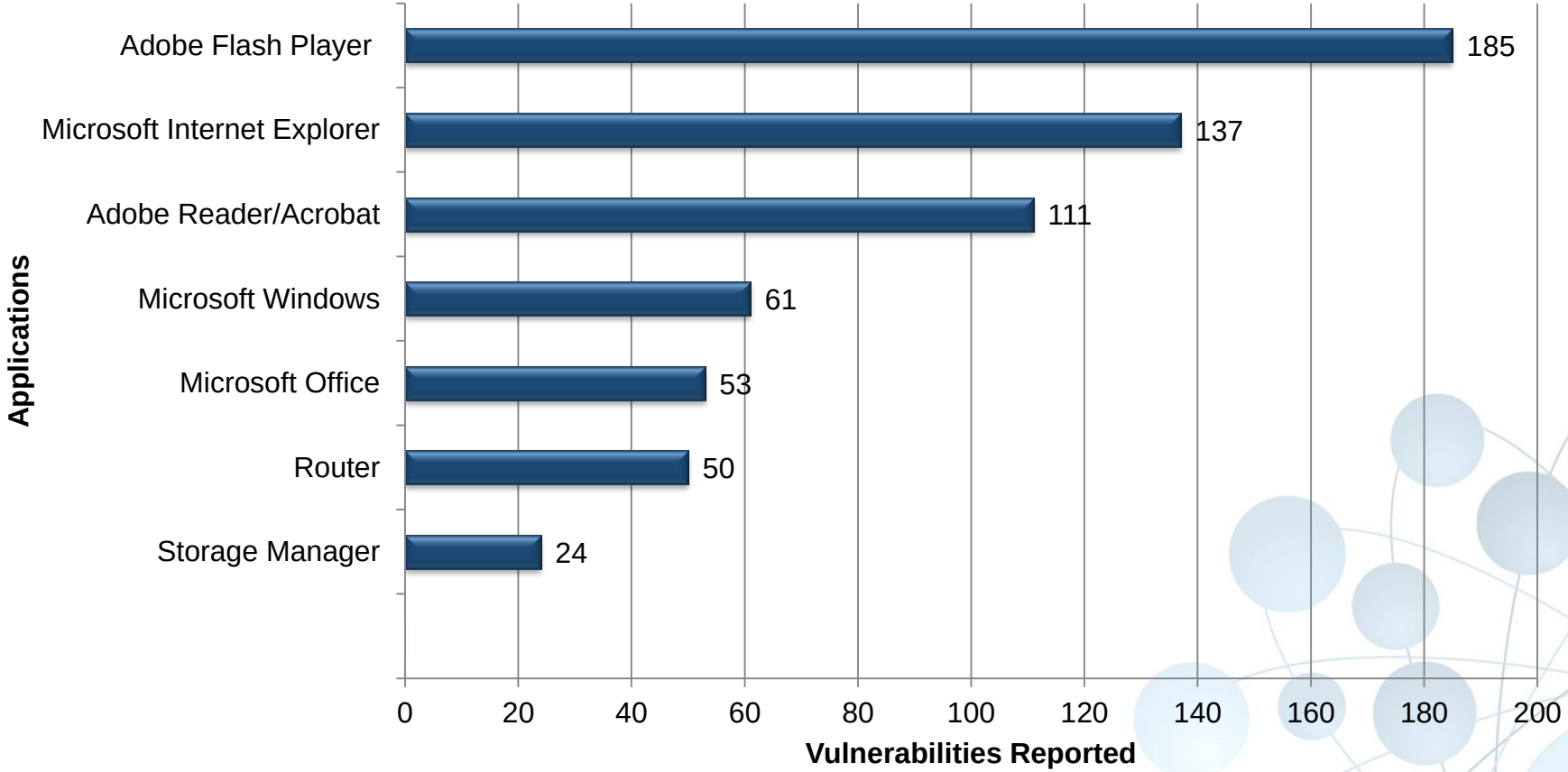
- Based on the total 1,337 vulnerabilities in 2015 that Frost & Sullivan included in this report:
  - Critical vulnerabilities were 277, a year-over-year increase of 82.2%, accounting for 20.7% share
  - High severity vulnerabilities of 540, a year-over-year increase 88.2%, accounting for 40.4% share
  - Medium severity vulnerabilities declined 32.7% to 297, accounting to 22.2% share
  - Low severity vulnerabilities increased 26.9% to 33, a share of 2.5%
  - Vulnerabilities that were not ranked totaled 190. This is an increase of 691.7% from 2014 and 14.2% of total vulnerabilities in 2015.
- Automated systems are being used for continuous diagnostics do a better job to remediate critical vulnerabilities. More organizations are making the transition from alert-based to analytics-enabled resulting in improved security operation processes.
- Overall in 2015 disclosing institutions and their partners, in particular Trend Micro ZDI and Google, have increased coverage of Critical and High severity vulnerabilities.

Source: Frost & Sullivan analysis.

Comparison of Targeted Applications

Targeted Applications

Public Vulnerability Research Market: Applications with the Highest Number of Unique Confirmed Vulnerabilities, Global, 2015



N=1,337 vulnerabilities

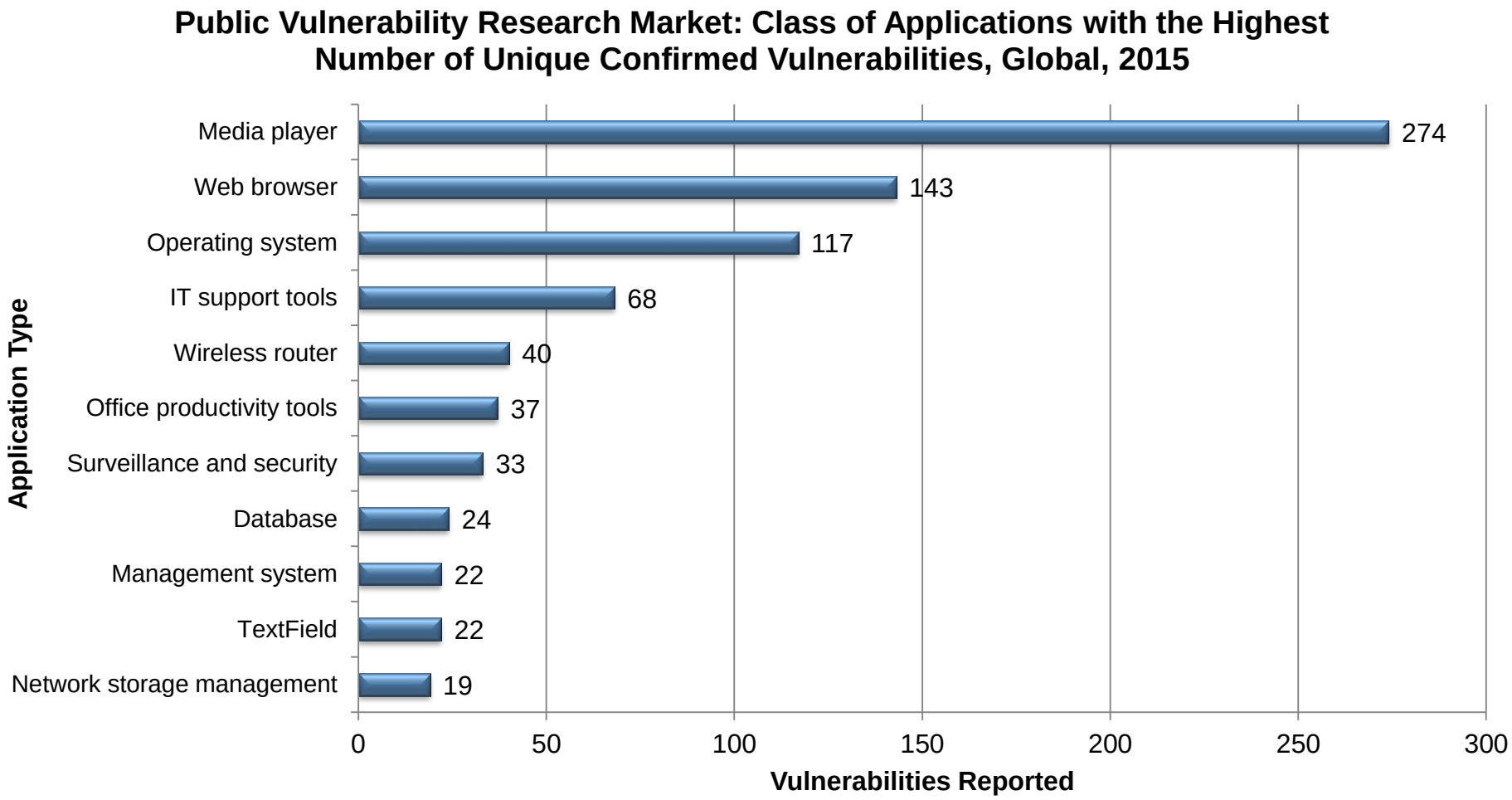
Note: All figures are rounded. The base year is 2015 Source: Frost & Sullivan analysis.

Analysis of Targeted Applications

- In 2015, in our study, the top five applications with the most vulnerabilities were: Adobe Flash Player, Microsoft Internet Explorer, Adobe Acrobat Reader, Microsoft Windows, and Microsoft Office.
- The biggest year-over-year leap was for Adobe Flash Player with 185 compared to 46 in 2014
- All editions of Microsoft Internet Explorer from 6 thru 11 have vulnerabilities. There were 137 vulnerabilities in 2015, down slightly from 143 in 2014.
  - Internet Explorer is not easily found in Windows 10. It is there, just not upfront. Unless the browser replacement, Microsoft Edge, is not as vulnerable, upgrades and new installs of Windows 10 might reverse this trend and further confirm Microsoft's decision to build a new browser.
- Adobe Acrobat Reader had 111 vulnerabilities, almost 5X more than the 23 in 2014.
- Adobe's products combined accounted for more than 22% of the vulnerabilities in 2015
- Client-side applications, particularly Web browsers, contained a large portion of reported vulnerabilities. However, pertaining to vulnerabilities with Microsoft Internet Explorer specifically, it is hard to tell what is cause and what is effect. Internet Explorer is a ubiquitous business and personal tool. Intuitively, it makes more sense to try to enter other data sources through the client-side rather than attack a network directly.
- The problem is that since researchers are independently looking for vulnerabilities on their own, it is possible that researchers are focusing on media applications, such as Adobe, and Internet Explorer because these are applications which are best known in their research domains.
- The applications noted above are the bulk of the vulnerabilities, but researchers are casting a wider net. In 2015 there were over 260 applications cited compared to 148 in 2014.

Source: Frost & Sullivan analysis.

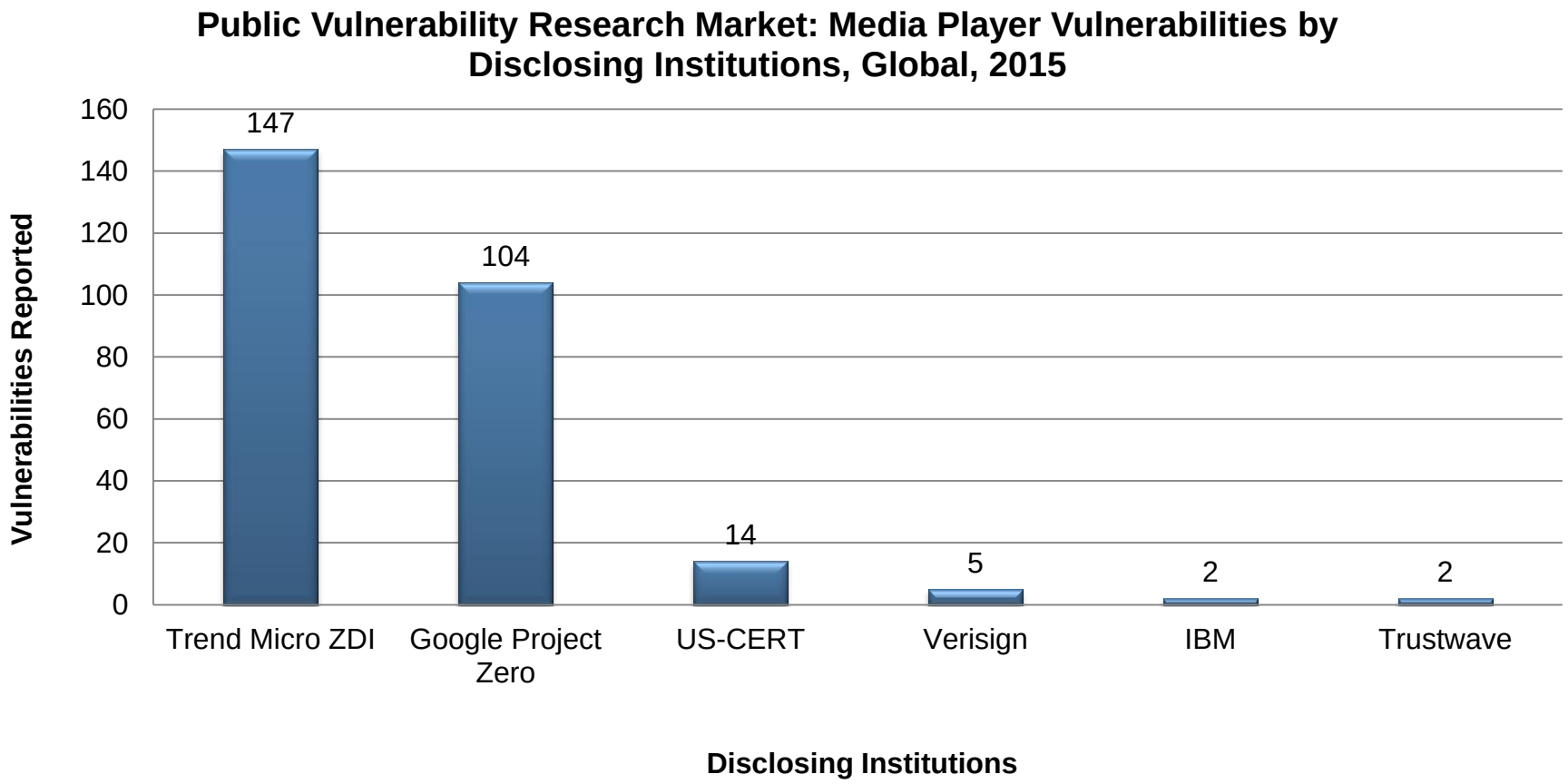
Top Targeted Class of Applications



N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

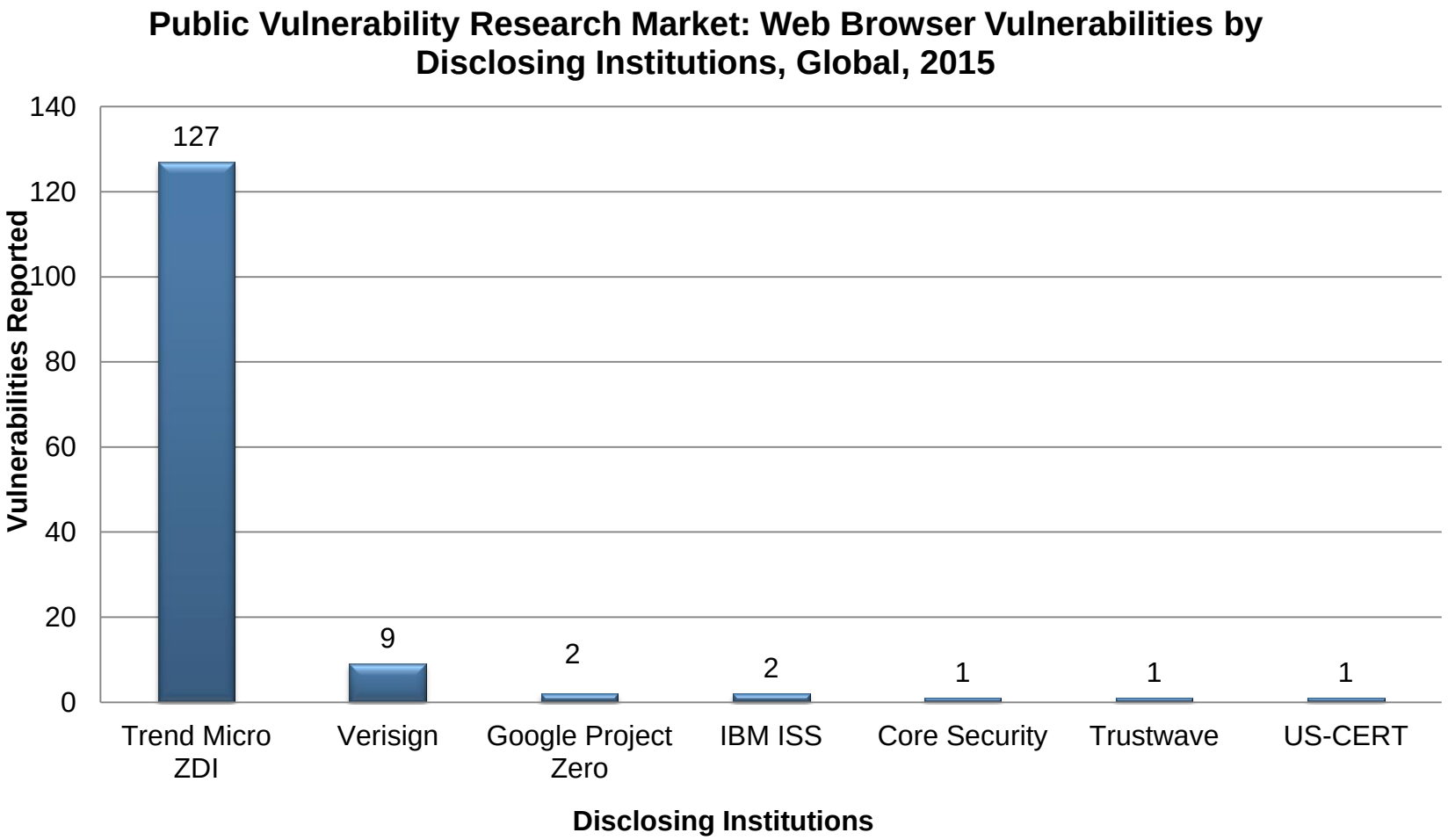
Disclosing Institutions: Media Player Vulnerabilities



N=274 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

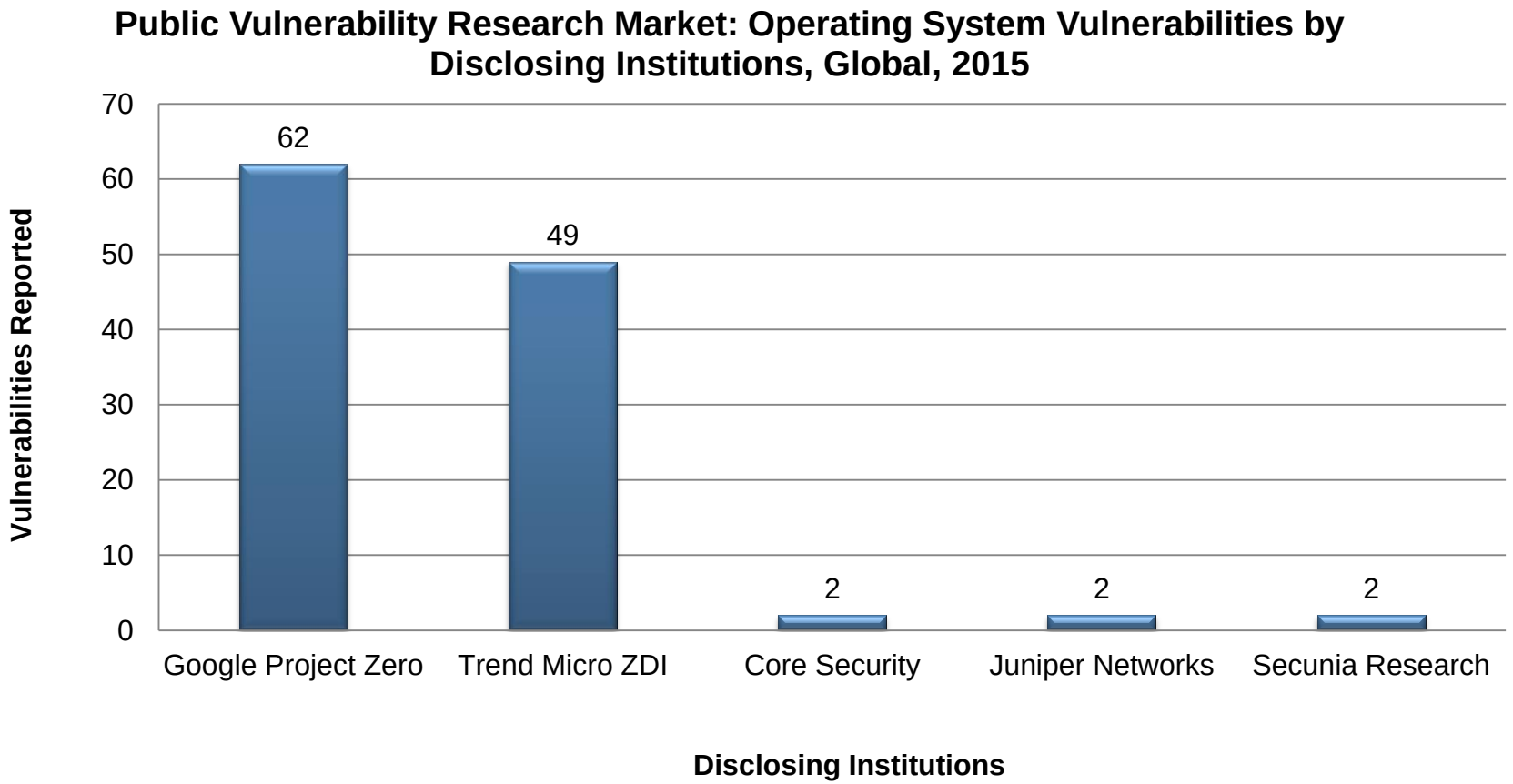
Disclosing Institutions: Web Browser Vulnerabilities



N=143 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

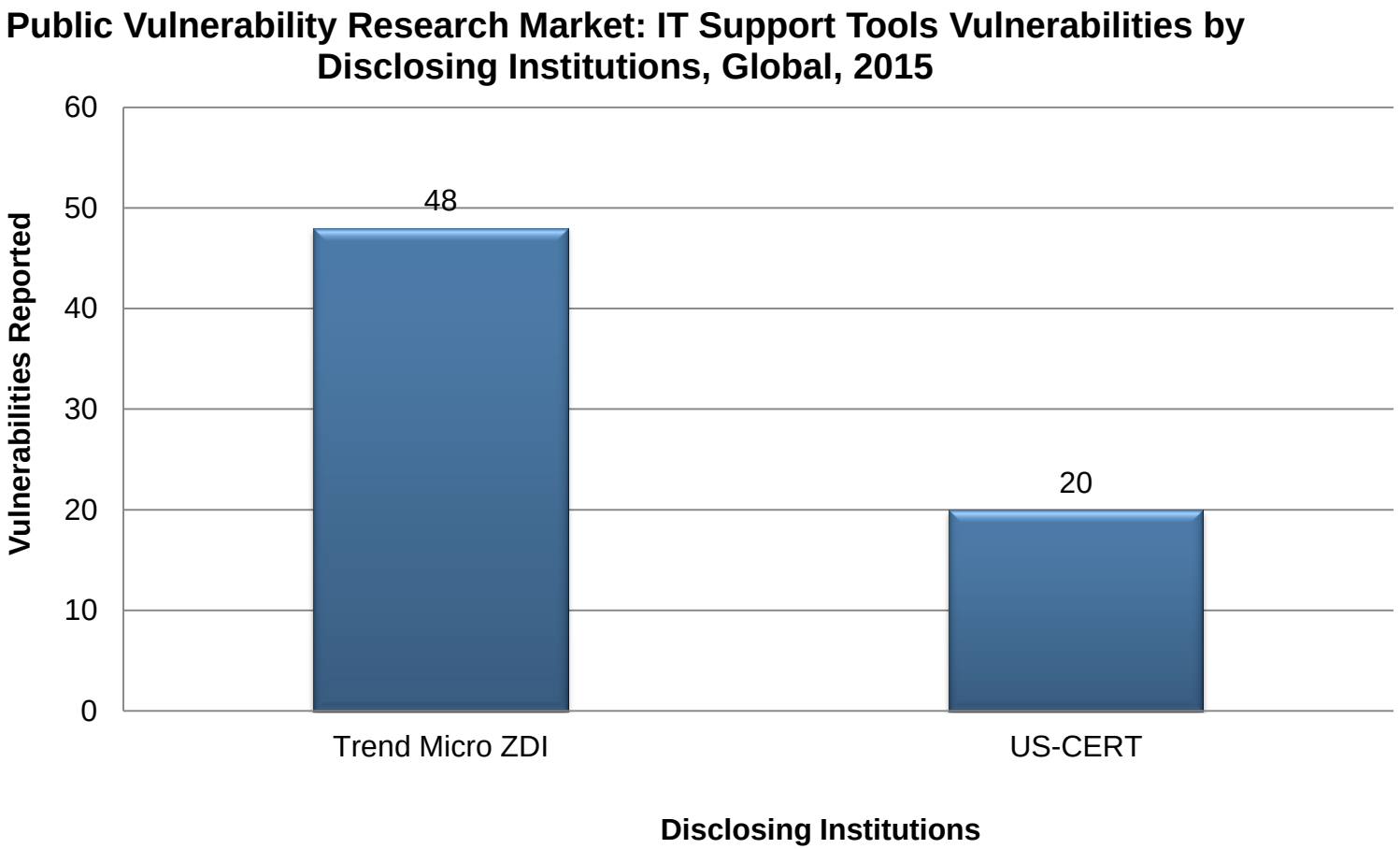
Disclosing Institutions: Operating System Vulnerabilities



N=117 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Disclosing Institutions: IT Support Tools Vulnerabilities



N=68 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Analysis of Targeted Applications by Class

- Media players had 274 vulnerabilities in 2015, with Adobe Flash accounting for the bulk of these. This represents 20.5% of total vulnerabilities. In 2014 media players had only 46 vulnerabilities, less than 5% of total vulnerabilities.
- Trend Micro ZDI was the leading disclosing institution for media players, with Google second.
- For the past few years most of the participating public vulnerability research firms made the observation that vulnerabilities have been migrating toward the Web and toward Web-based applications. In 2015 this observation appears to be changing. Frost & Sullivan found 207 vulnerabilities (or 15.5% of all vulnerabilities) directly related to Web applications. However, in 2014 Web-based applications were 273 vulnerabilities, accounting for 29.4%
- The Web browser was the most targeted application within Web applications with 147 discovered vulnerabilities. Web servers accounted for 24 vulnerabilities.
- The Web browser is especially problematic. The most current available Microsoft Web browser is Microsoft Internet Explorer (IE) version 11. IEv6 through IEv11 are largely backward and forward compatible, however, largely is the operative word. In many cases, an application in IEv9 is not compatible with IEv11. If an application based on an IE9 browser will function in IEv11, the update to the newest browser will likely not be undertaken by organizations that depend on the IEv9-supported applications.
- Trend Micro ZDI was the dominant disclosing institution for Web browser vulnerabilities.

Source: Frost & Sullivan analysis.

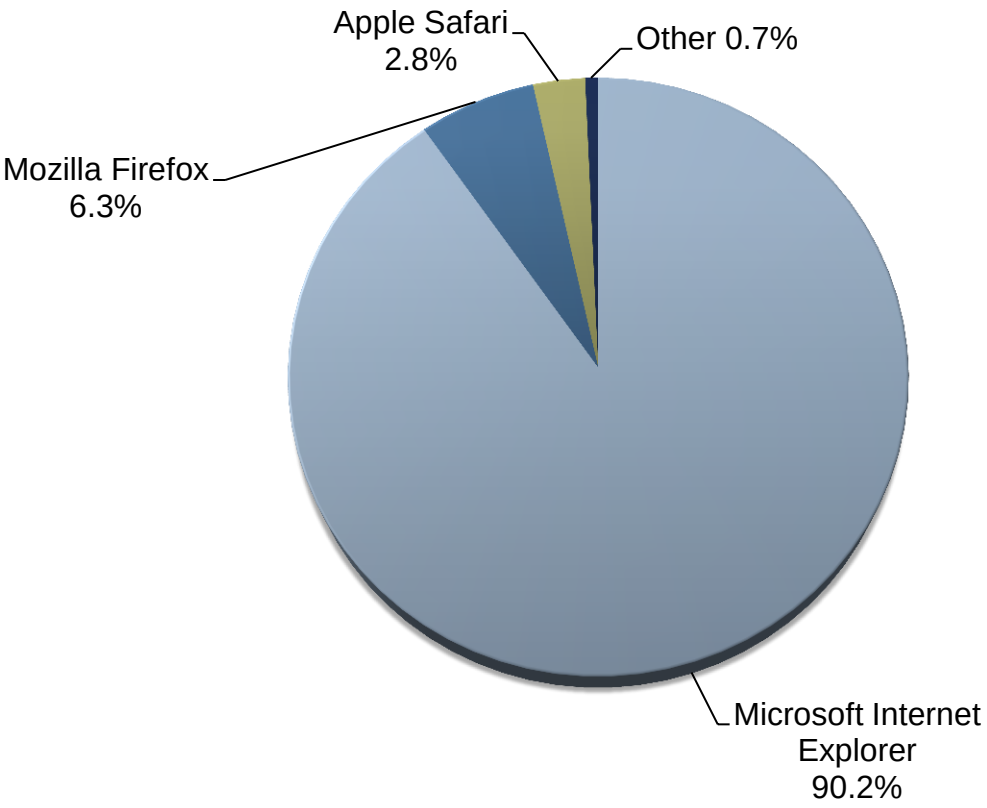
Analysis of Targeted Applications by Type (continued)

- Operating systems were the third highest with 117 vulnerabilities. These are predominantly various versions of Microsoft Windows. In 2014 operating systems had only 32 reported vulnerabilities. Researchers have been focusing more attention in this area.
- Google and Trend Micro ZDI were the dominant disclosing institutions for operating systems.
- Various applications constituting IT support tools had 68 vulnerabilities. In 2014, there were no IT support tools cited.
- Trend Micro ZDI and US-CERT are the only two disclosing institutions for IT support tools. Trend Micro ZDI accounts for more than two-thirds of the reporting.
- Wireless router vulnerabilities were 40 in 2015, this is double the number in 2014. Most of the issues are with the firmware.
- Office productivity tools include Microsoft Office Suite, in particular, Word and Excel.

Source: Frost & Sullivan analysis.

Targeted Web Browser Type

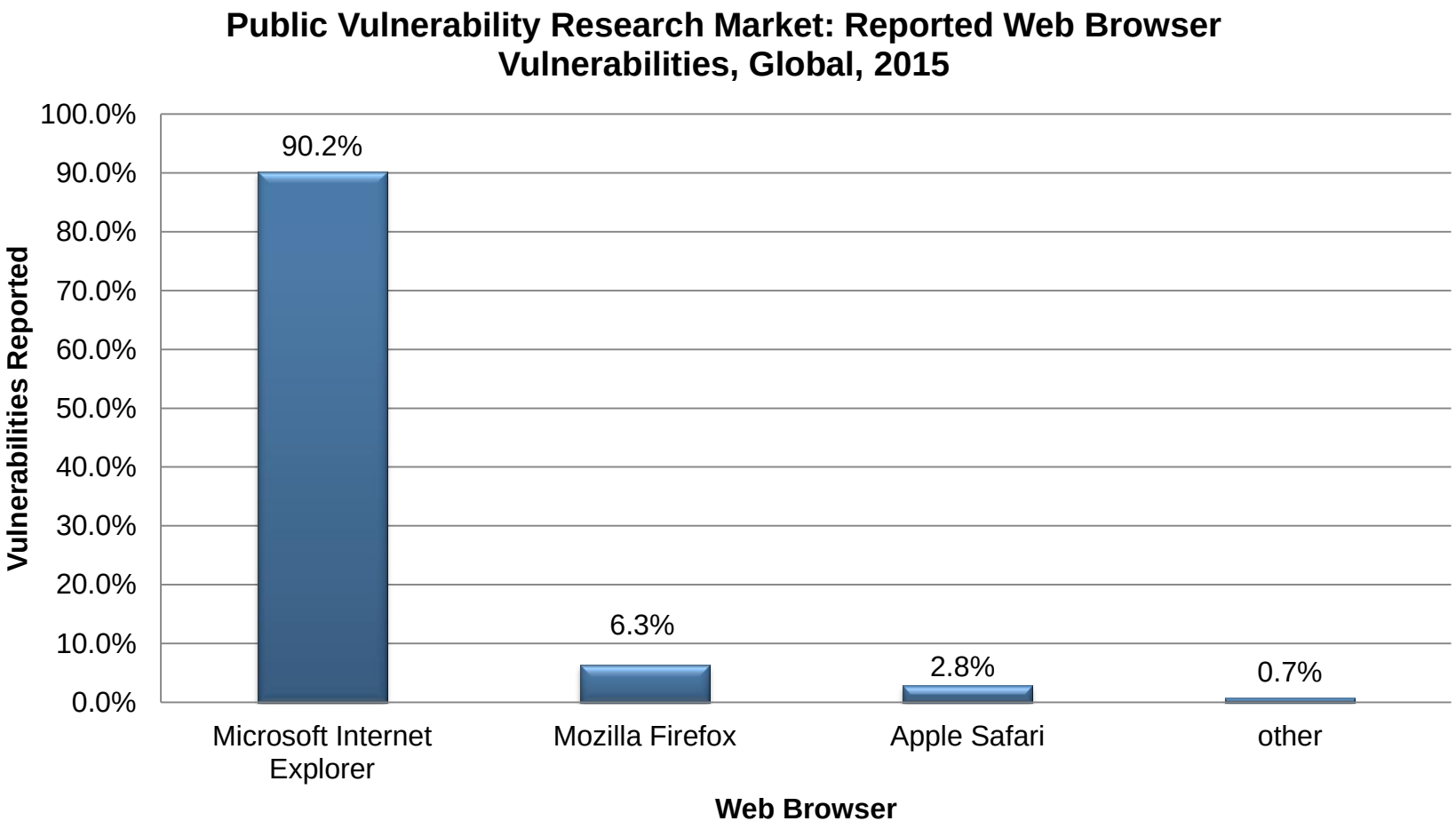
Public Vulnerability Research Market: Percent of Reported Vulnerabilities by Web Browser Type, Global, 2015



N=143 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Targeted Web Browser Type (continued)



N=143 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Analysis of Targeted Web Browser Type

- In 2015, Microsoft Internet Explorer had the most publicly reported vulnerabilities with 129. This was down from the 143 reported in 2014.
- Mozilla Firefox was a distant second with 9 vulnerabilities in 2015. This is essentially flat compared to the 8 vulnerabilities in 2014.
- Web browsers were 147 of 207 attributed to Web-based vulnerabilities.
- As note previously, researchers are casting a wider net. More different classes of applications are being examined. In 2015 there were 196 classes encompassing the 1,337 vulnerabilities. This is an increase over the 103 classes in 2014.

Source: Frost & Sullivan analysis.

Vulnerability Analysis

Vulnerability Definitions

This research study references Common Weakness Enumeration (CWE) specifications to describe vulnerability flaw types. Definitions of the most frequently occurring vulnerabilities in 2015 are as follows:

- **Buffer errors** - A memory buffer is a memory slot of a specific, allocated size. Hackers can assign too much data in the memory buffer, which will cause data to spill into other memory slots, resulting in application crashes or malfunctions.
- **Use After Free** - Referencing memory after it has been freed can cause a program to crash, use unexpected values, or execute code.
- **Permissions, privileges, and access** - Errors relating to permissions, privileges, and access occur when a program provides too much access or rights to unauthorized parties.
- **Information Leak / Disclosure** - An information exposure is the intentional or unintentional disclosure of information to an actor that is not explicitly authorized to have access to that information.
- **Improper input validation** - Improper input validation occurs when a program accepts incorrectly formatted data as valid user input. Attackers can then input data that the program cannot handle, causing the application to crash or act improperly.
- **Resource management errors** - These errors occur when a program does not limit the amount of resources, such as memory or processing power, that it uses. Attackers can then use up all the system's resources to block system access by legitimate users.

Source: National Vulnerability Database. Common Weakness Enumeration. http://nvd.nist.gov/cwe.cfm#cwes; Frost & Sullivan.

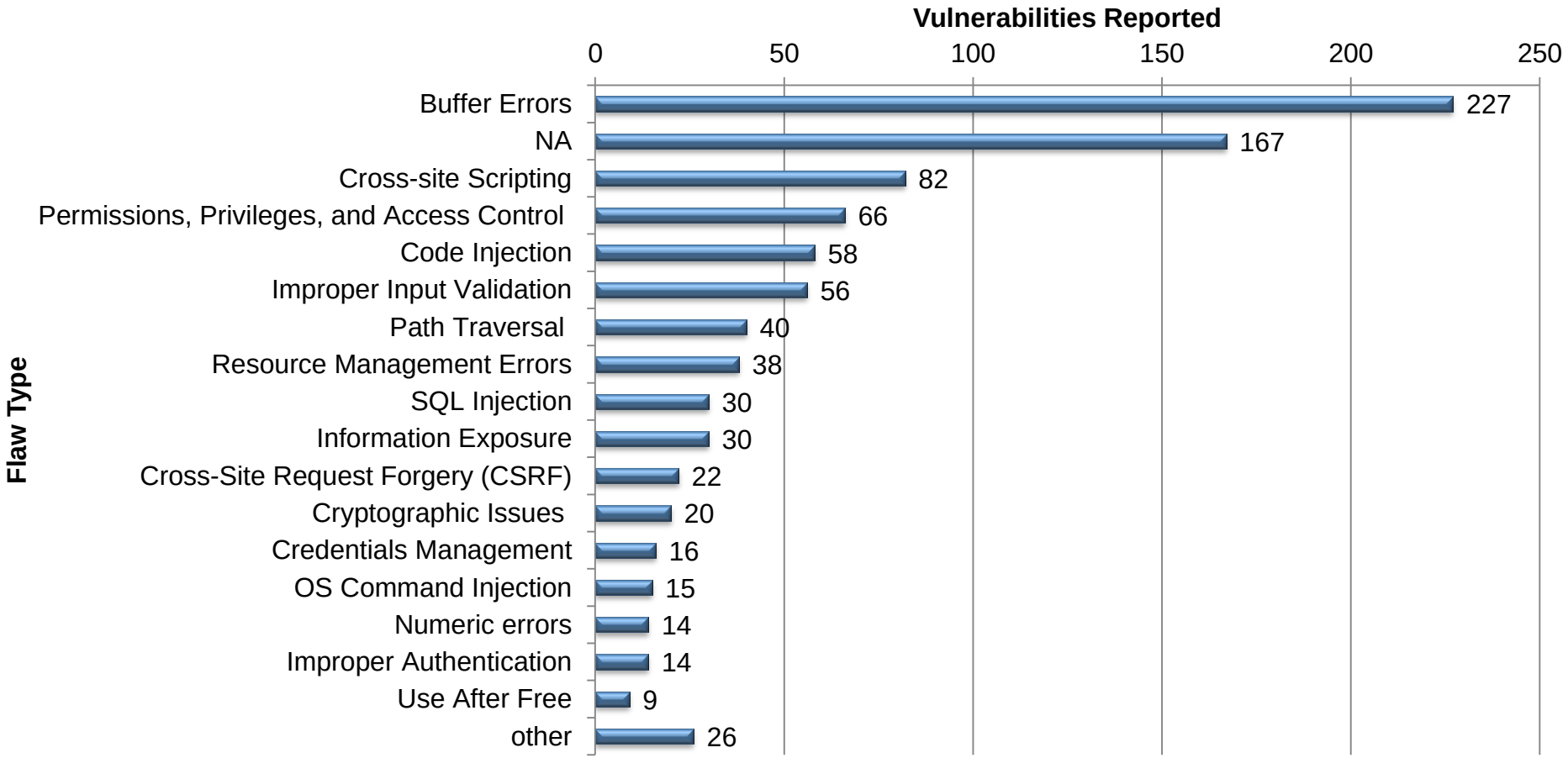
Vulnerability Definitions (continued)

- **Numeric errors** - Many programs must be able to conduct precise mathematical calculations. When programs do not accurately handle numbers, such as when rounding errors or changing number signs, the program's accuracy will be compromised.
- **Cross-site scripting (XSS)** - Cross-site scripting occurs when a Website does not validate or protect a user's data before passing it to another user. Attackers can use this high-speed malware on Web pages.
- **Code injection** - Code injection occurs when a third-party code infiltrates a program's legitimate code. This type of vulnerability allows attackers to control and manipulate a system.
- **SQL injection** - SQL injection enables attackers to execute code and control a database in an unauthorized manner. Vulnerabilities in Websites or Web applications enable the attacker to inject code into the database, which allows the user to control the system.
- **Cryptographic issues** - Cryptography is a set of algorithms that render data indecipherable to unauthorized users. Authorized users are provided with the key to decrypt and read the data. These systems may be vulnerable to attacks that bypass or obtain unauthorized access to the key.
- **CSRF** - Cross-site request forgeries enable attackers to act as a particular end user and perform unauthorized actions. CSRF attacks rely on authorization and authentication data that has been saved by a user's browser to perform actions under the user's approval.

Source: National Vulnerability Database. Common Weakness Enumeration. http://nvd.nist.gov/cwe.cfm#cwes; Frost & Sullivan.

Vulnerabilities Reported by Flaw Type (2014)

Public Vulnerability Research Market: Reported Vulnerabilities by Top Flaw Type, Global, 2014

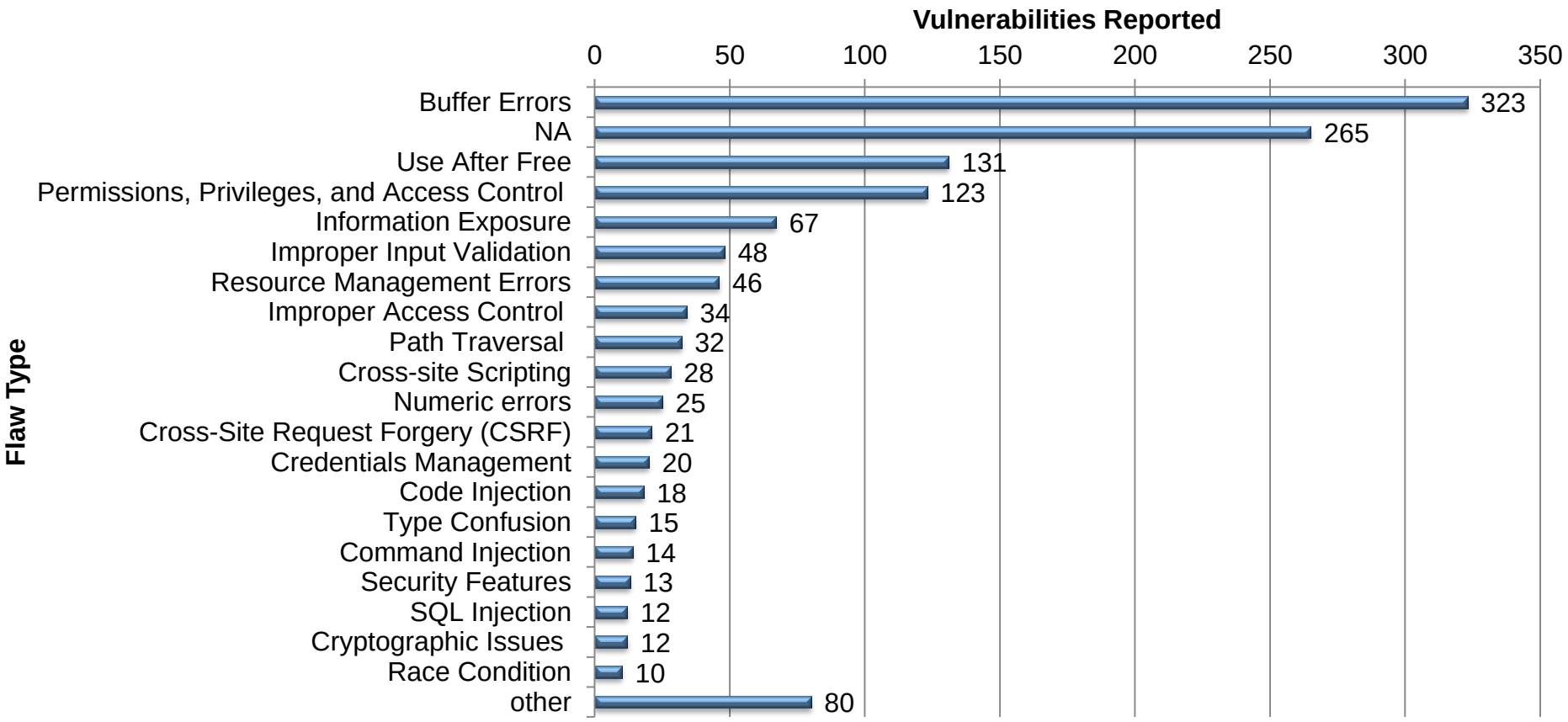


N=930 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Vulnerabilities Reported by Flaw Type (2015)

Public Vulnerability Research Market: Reported Vulnerabilities by Top Flaw Type, Global, 2015

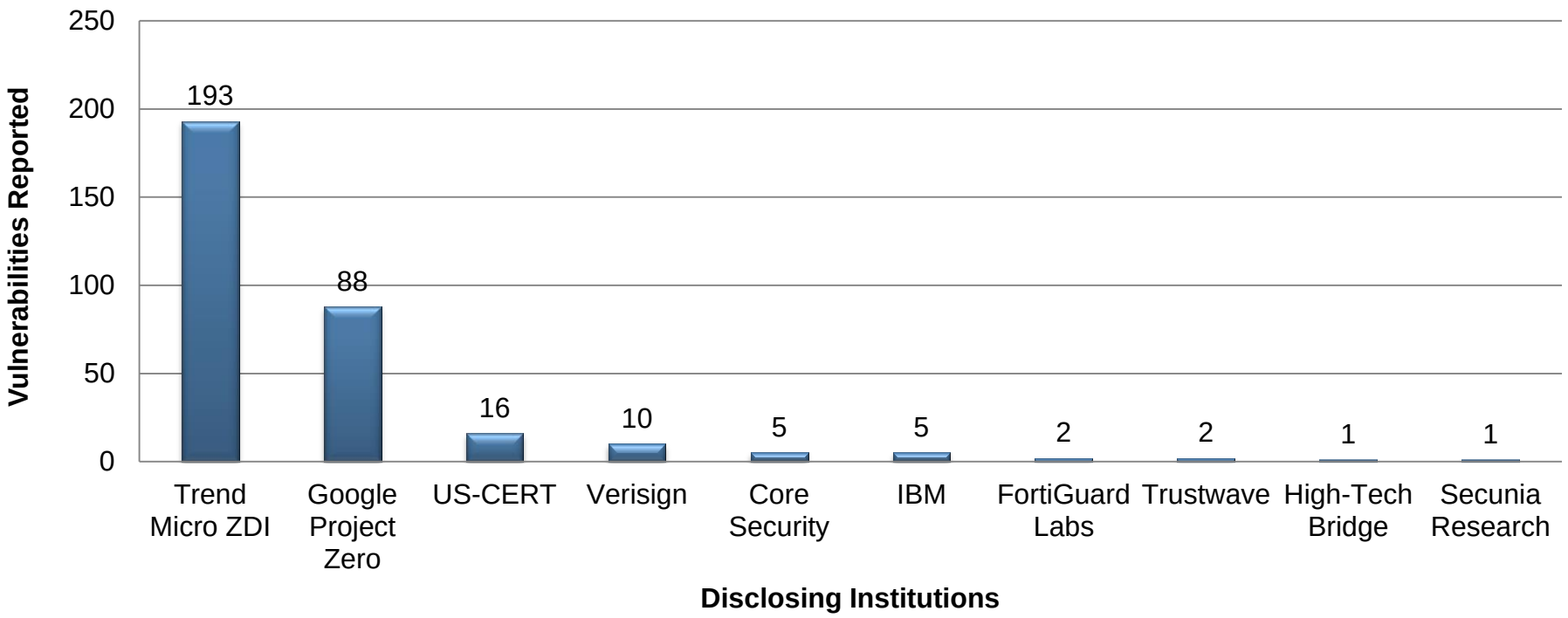


N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Disclosing Institutions: Buffer Errors

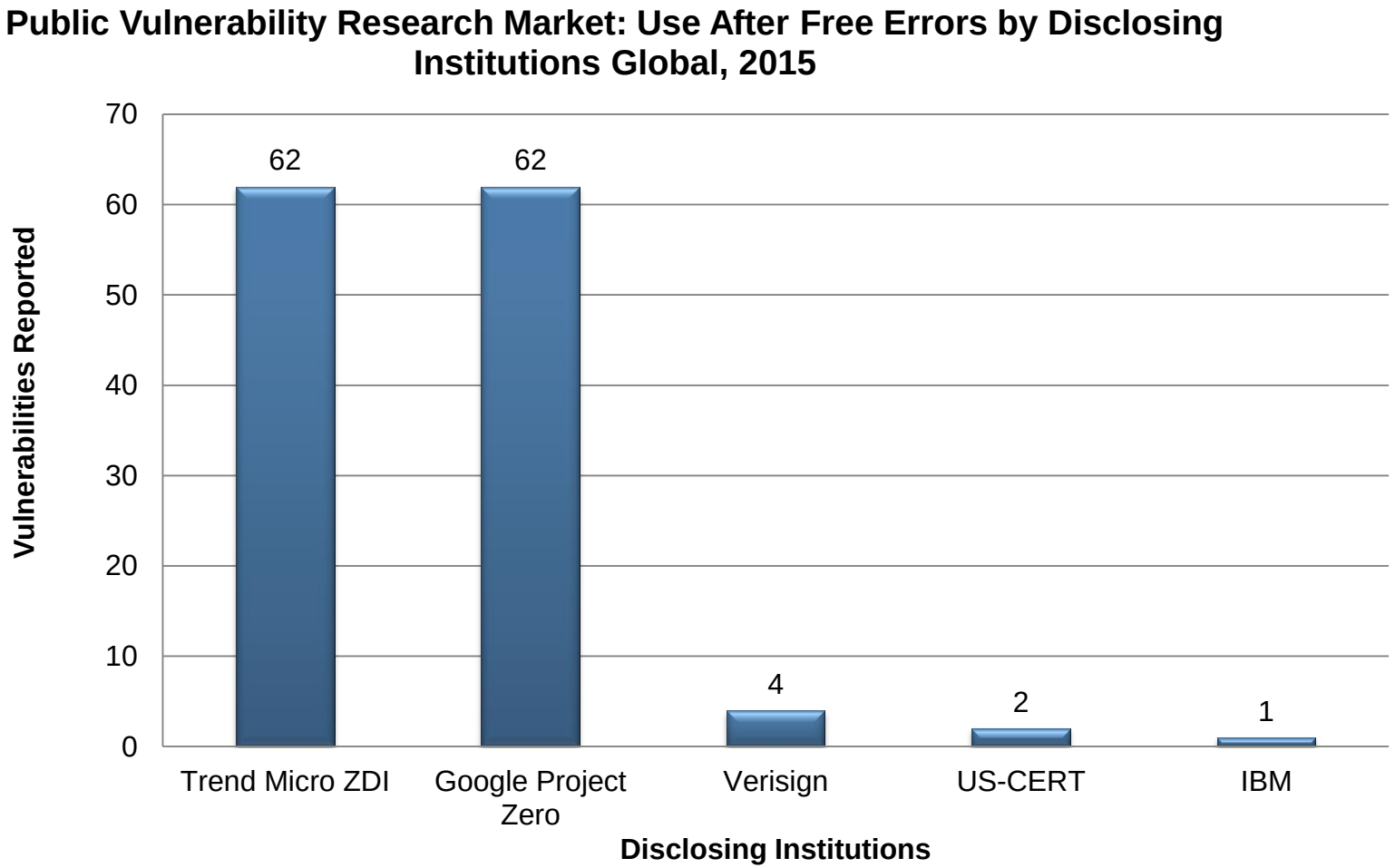
Public Vulnerability Research Market: Reported Buffer Errors by Disclosing Institutions Global, 2015



N=323 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

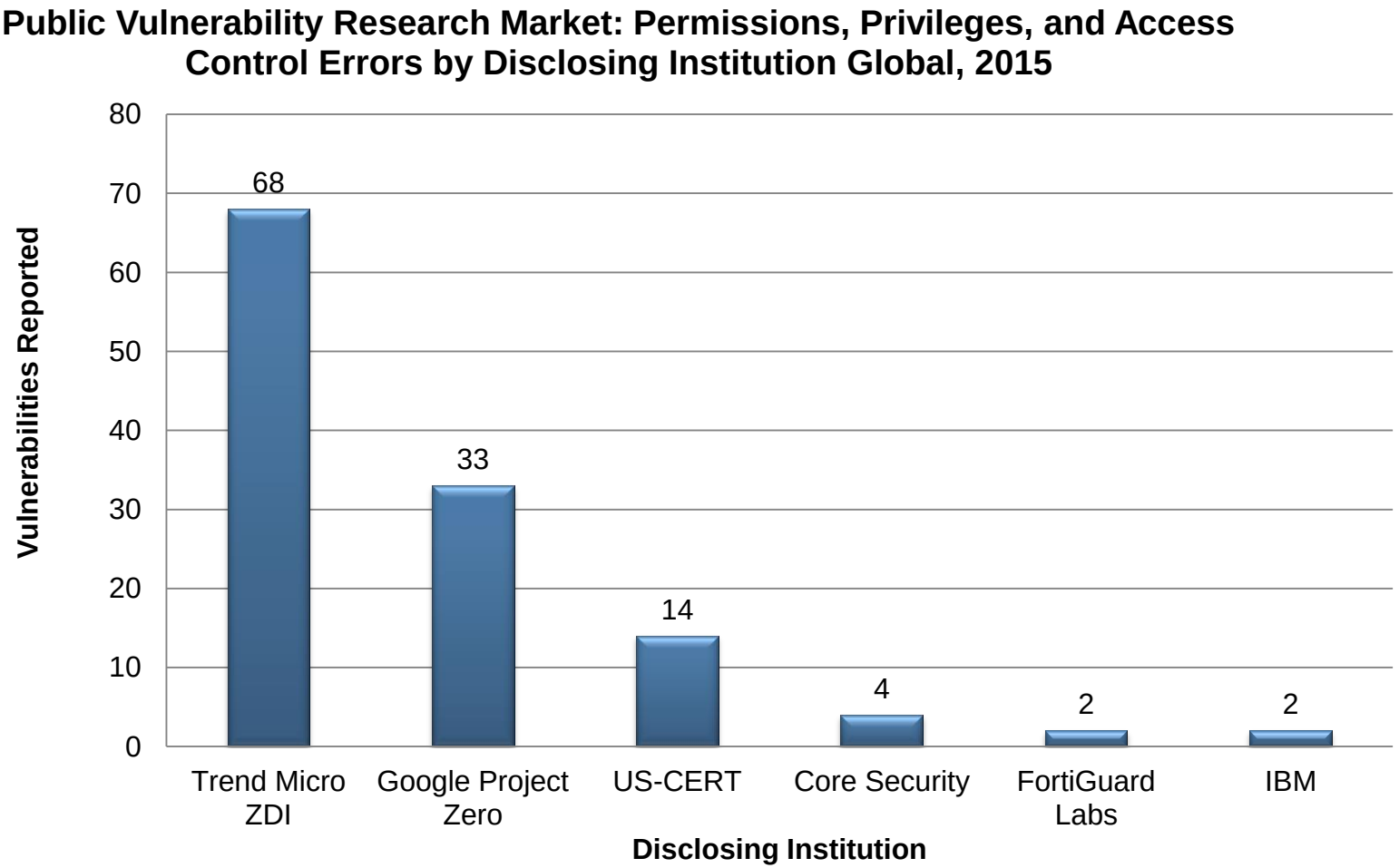
Disclosing Institutions: Use After Free Errors



N=131 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Disclosing Institutions: Permissions, Privileges, and Access Control Errors

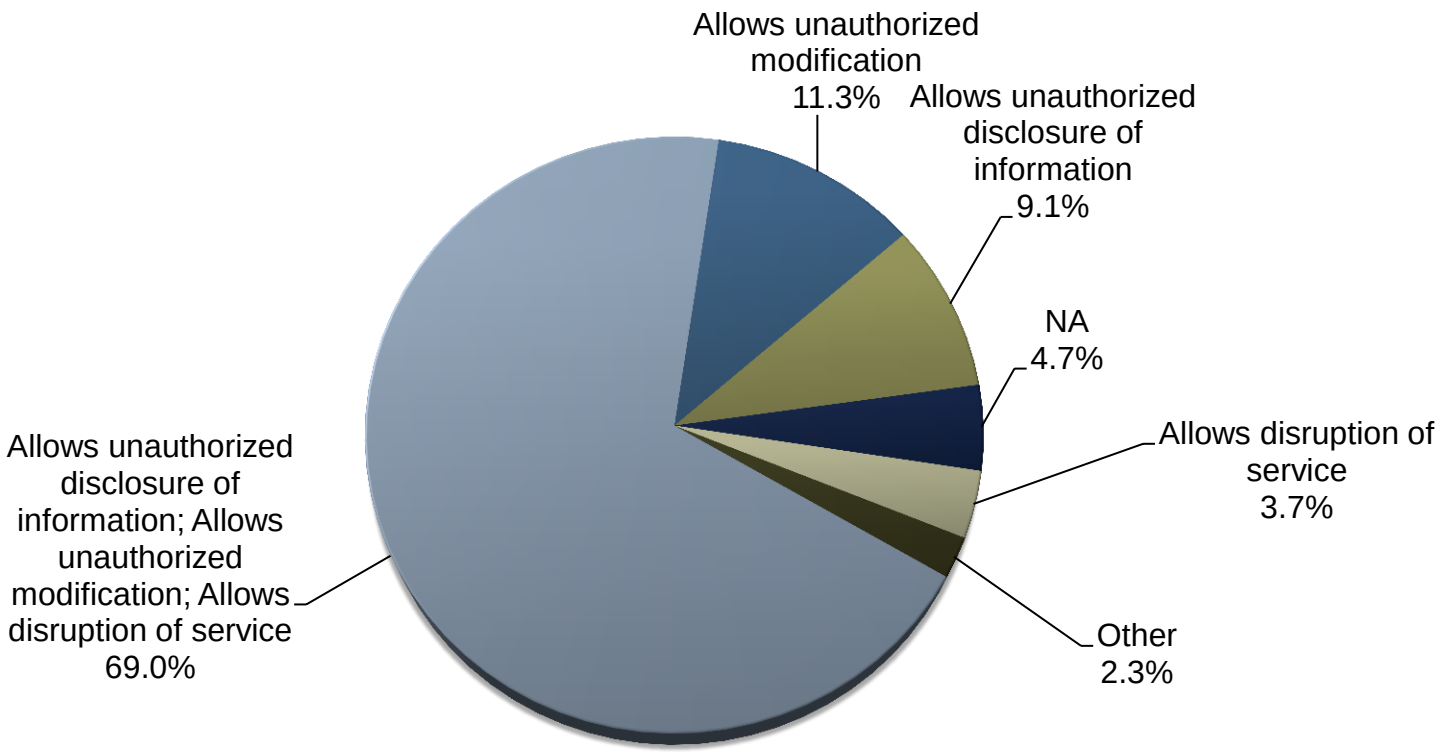


N=123 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Top Impact Type (2014)

Public Vulnerability Research Market: Percentage of Vulnerability Reports by Associated Impacts, Global, 2014

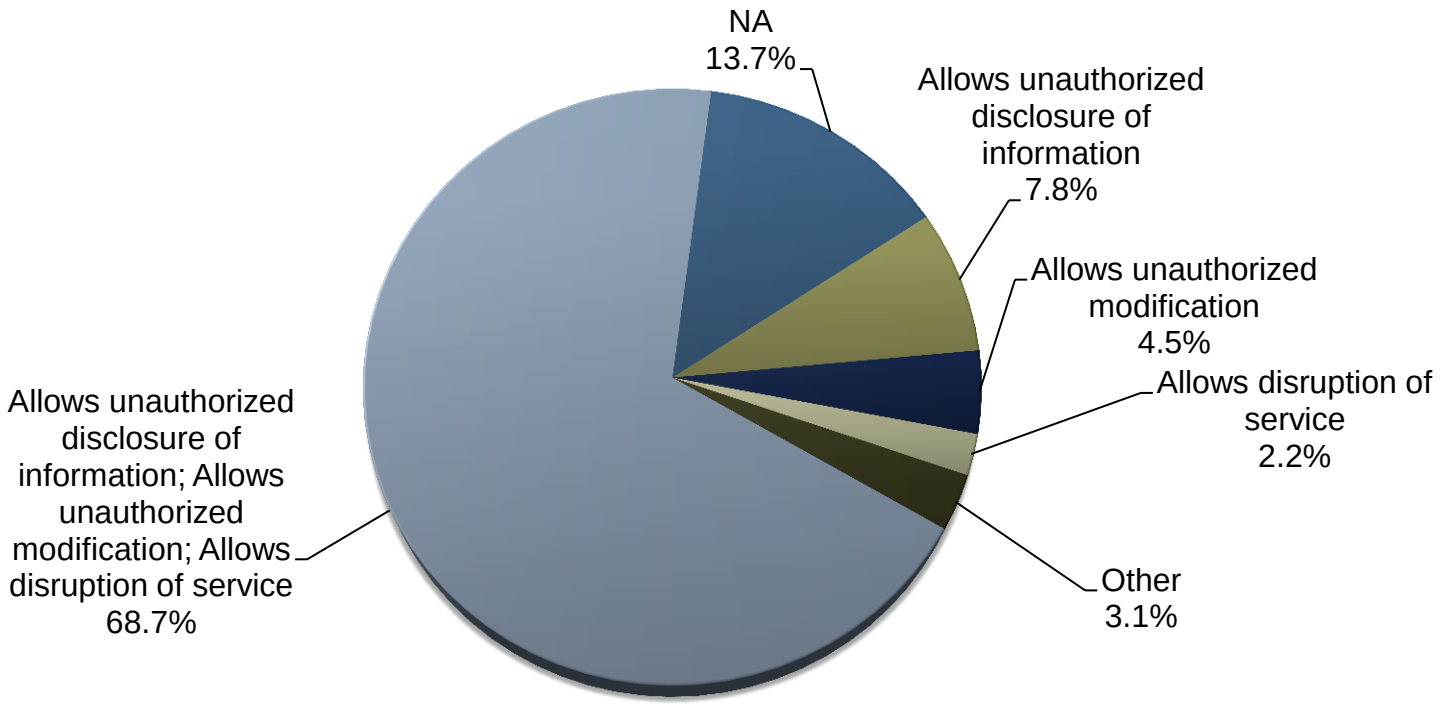


N=930 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Top Impact Type (2015)

Public Vulnerability Research Market: Percentage of Vulnerability Reports by Associated Impacts, Global, 2015

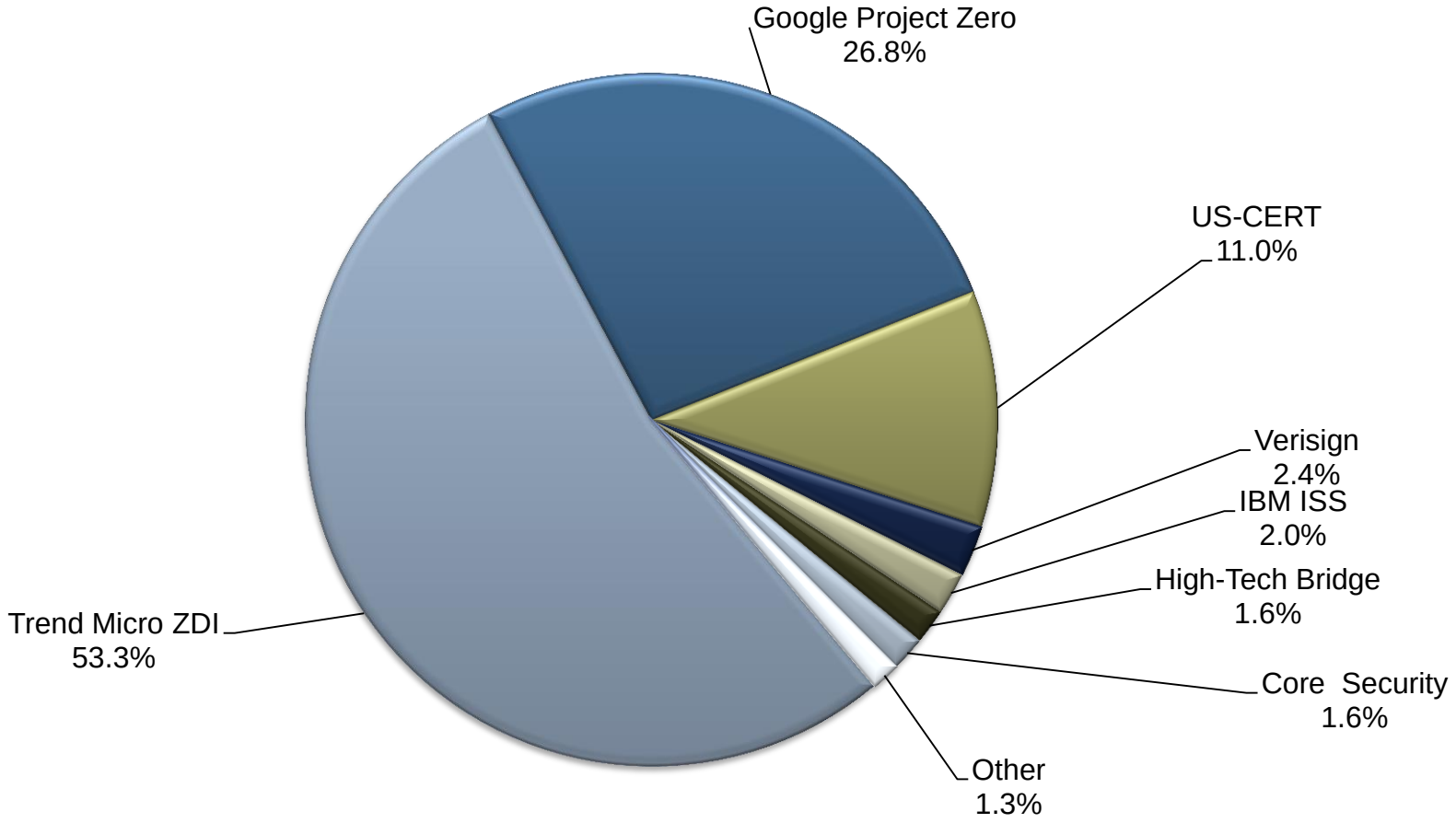


N=1337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Disclosing Institution: Disruption-of-Service/Unauthorized Modification/Disclosure of information Impacts

Public Vulnerability Research Market: Disruption-of-Service/Unauthorized Modification/Disclosure of information Impacts by Reporting Source, Global, 2015



N=919 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

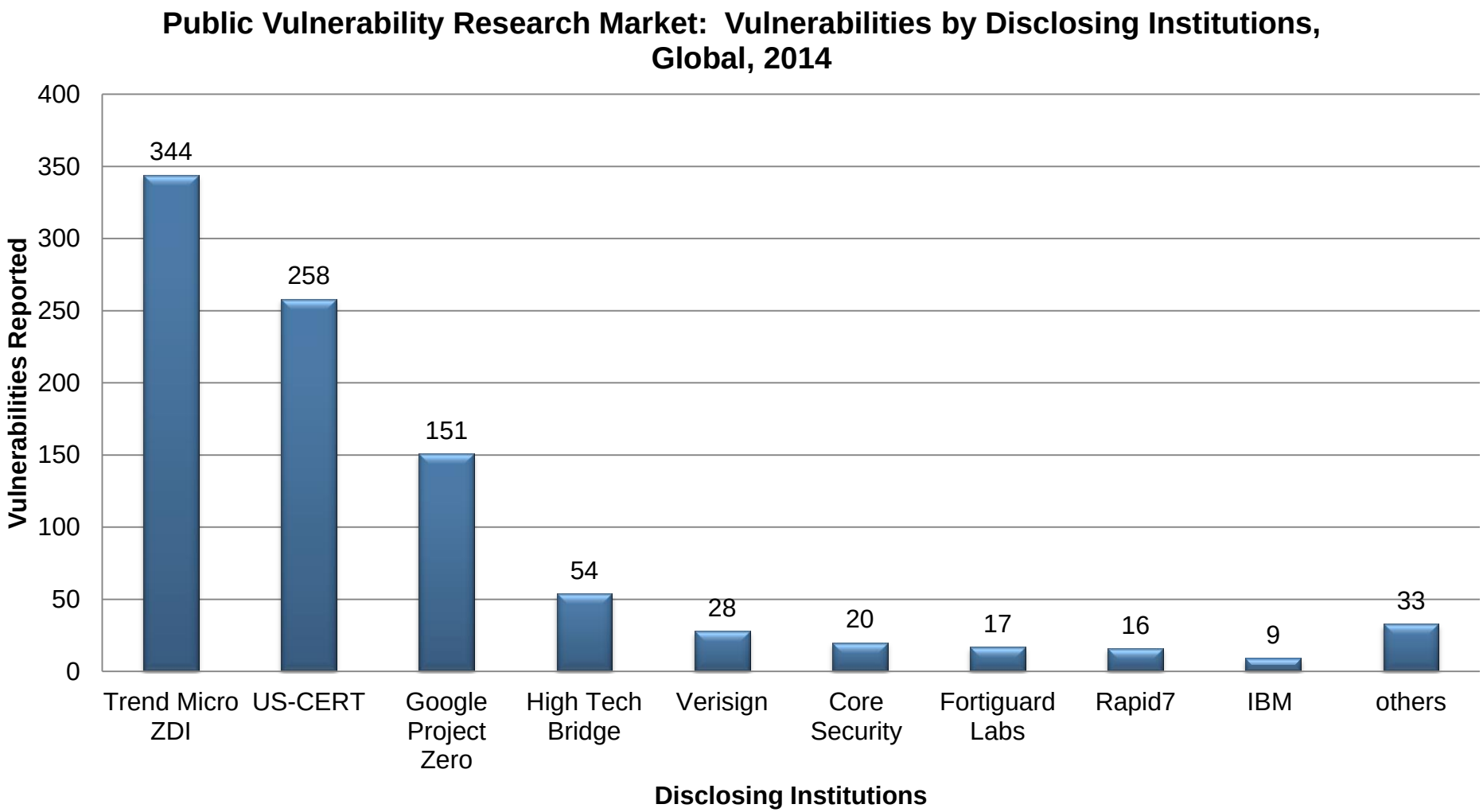
Analysis of Impact Types

- The NVD was the final authority used to report the impacts in the tables.
- Buffer overflow errors were the most common vulnerability flaw in 2014 and remained so in 2015. Trend Micro ZDI found 193 incidents of buffering errors in 2015, followed Google which found 88 vulnerabilities related to buffering errors.
- Interestingly, the NVD determined there were 265 vulnerabilities where a known vulnerability flaw could not be ascribed to a potential exploit.
- Use After Free (131 vulnerabilities), Permissions, Privileges, and Access Control (123 vulnerabilities), Information Exposure (67 vulnerabilities), Improper Input Validation (48 vulnerabilities) and Resource Management Errors (46 vulnerabilities) were the next most common vulnerability flaws.
- If a vulnerability was found, 68.7% of the time the impact was likely to be exploited to deny service, modify files and allow unauthorized access (919 vulnerabilities could be subject to all three impacts). This could be classified as a jailbreak vulnerability.
- Trend Micro ZDI found 53.3% of all of the jailbreak vulnerabilities discovered by public vulnerability reporting organizations.

Source: Frost & Sullivan analysis.

Competitive Analysis

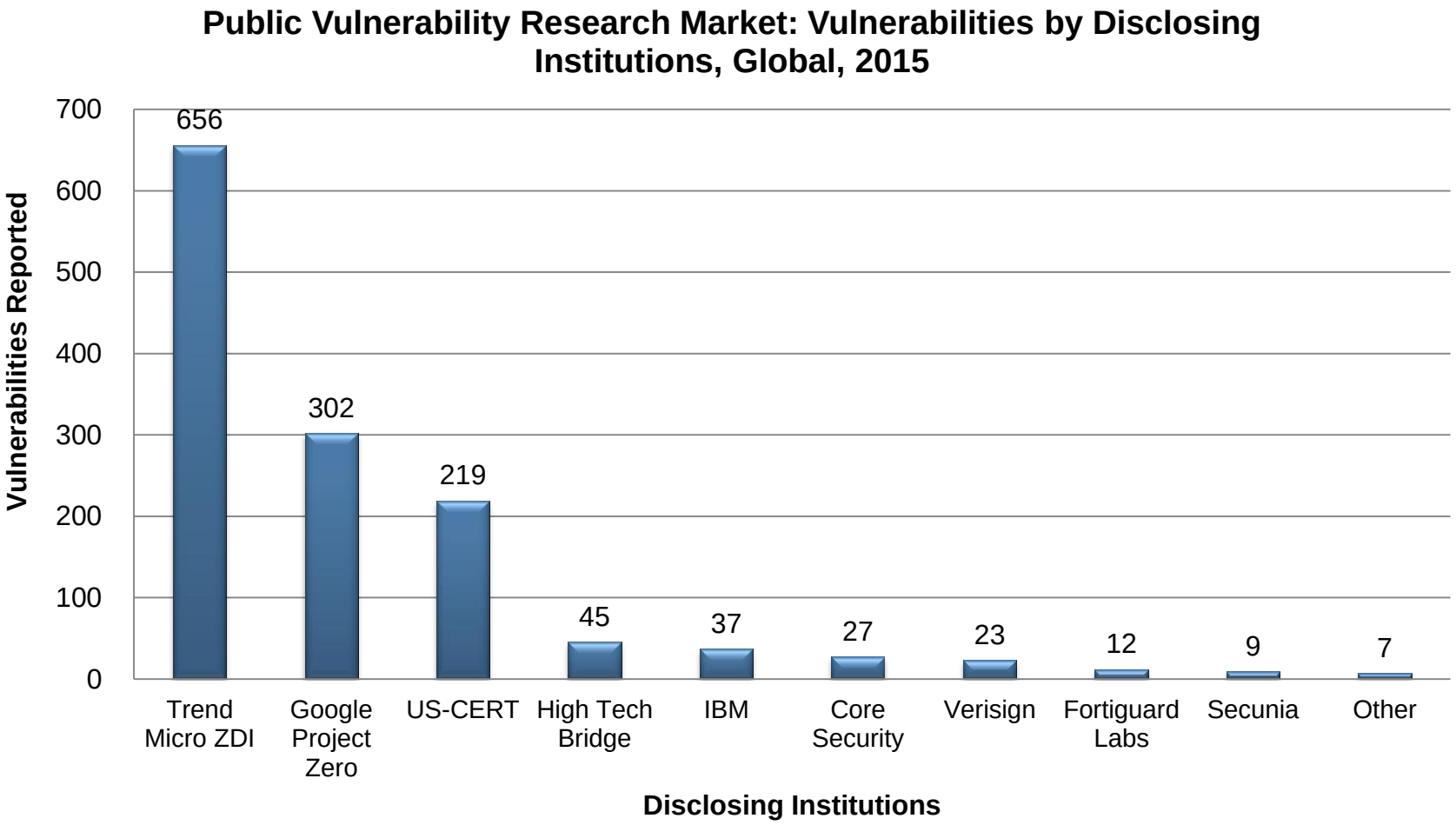
Competitive Analysis Vulnerabilities



N=930 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Competitive Analysis Vulnerabilities (continued)

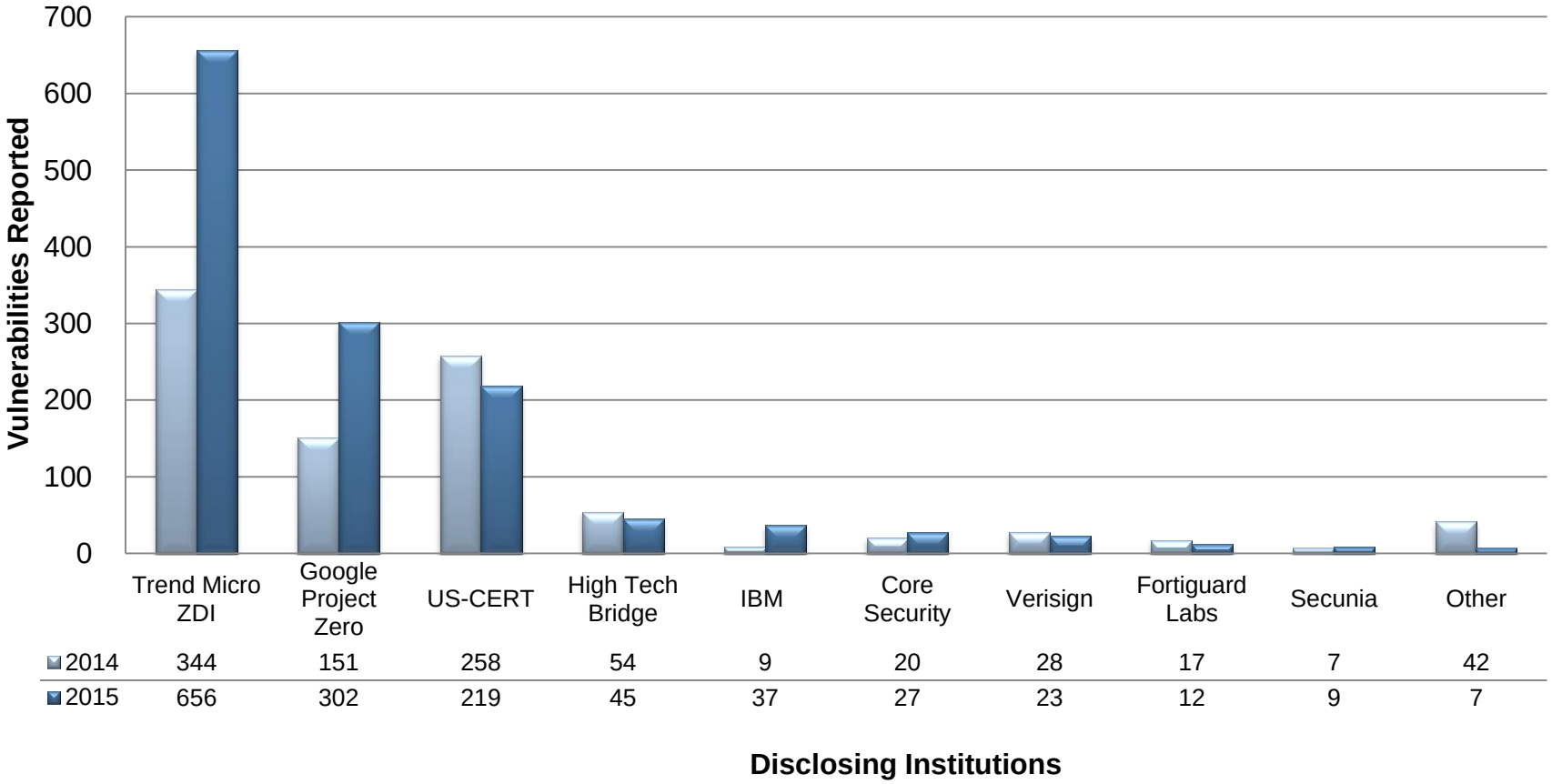


N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Competitive Analysis Vulnerabilities (continued)

Public Vulnerability Research Market: Total Vulnerabilities by Disclosing Institutions, Global, 2014 and 2015



N=1,337 vulnerabilities

Note: All figures are rounded. The base year is 2015. Source: Frost & Sullivan analysis.

Competitive Analysis (continued)

- Frost & Sullivan uses only verified vulnerabilities in the formal competitive analysis.
  - A vulnerability is considered “verified” once it is issued a CVSS temporal score by NVD. Worth noting, the CVSS score represented in an advisory does not always match the final score issued by NVD.
  - The requirement for verified vulnerabilities ensures that the data presented here is free from duplicate or rejected entries.
  - The most likely reason a vulnerability remains unverified is that the NVD could not prove a vulnerability exists, possibly due to insufficient exploit code.
  - Another possibility is that the NVD may not have tested the vulnerability by the time of publication. The NVD may require up to six months to test and issue a CVSS score but there are occasions when this process takes longer.
- In 2015, Trend Micro ZDI reported the most verified vulnerabilities with 656. This is a growth of 90.7% over the 344 reported in 2014. Trend Micro ZDI reported 49.1% of total vulnerabilities.
- Google Project Zero follows with 302 vulnerabilities in 2015, 100% growth over 2014 and 22.6% share in 2015. Google Project zero launched mid-2014.
- In terms of verified vulnerabilities in 2015, US-CERT reported 219, High-Tech Bridge is next with 45, and IBM with 37.

Source: Frost & Sullivan analysis.

The Status Of Public Vulnerability Reporting

The Status of Public Vulnerability Reporting—Then, Now, and in the Future

- From 2000–2011 (roughly), many companies offered public vulnerability reporting.
- Frost & Sullivan believes there were two primary motivations for this.
  - The number of vulnerabilities that were reported could be seen as direct evidence of the efficacy of what a vendor's security tool was finding. For example, in 2011 Secunia Research Advisories posted 225 advisories describing 435 vulnerabilities.
  - Secondly, the technically savvy people that are often referred to as "first adaptors" are passionate about technology. The thinking of security tools providers is that techies and ethical hackers would try to infiltrate networks, devices, and applications anyway. Why not offer a financial incentive and notoriety for the enthusiasts? In an odd way, public vulnerability report presaged social media.
- While Trend Micro Zero Day Initiative, Google Project Zero, and the US CERT still have significant public vulnerability reporting capabilities many companies have fallen off or simply do not publish as many advisories.
- In 2013, BeyondTrust and VUPEN discontinued their public vulnerability reporting practices. Secunia, and Verisign have smaller PV advisory footprints than in 2013. IBM X-Force has changed its methodology to offer more threat-centric reporting than just reporting CVE numbers.
- The problem with public vulnerability disclosure is that it is onerous and requires ownership. PV reporting requires a mechanism where the vulnerabilities are vetted for accuracy, relayed to PSIRT teams, and then properly posted on a Website.
- While the described lattice-work is detailed, the processes requires individuals on the payrolls of companies to take ownership of the reporting process as well as the formal payout to individual contributors. On a company-by-company basis, skilled security professionals are in high demand and assigning one to run a PV disclosure program may not be the best allocation of resources.
- Understand that this does not mean that there is less vulnerability research—far from it. Vulnerability research is the underpinning of all commercial threat cyber defense platforms.

Source: Frost & Sullivan analysis.

The Status of Public Vulnerability Reporting—Then, Now, and in the Future (continued)

- In vulnerability management, companies like Beyond Trust, Beyond Security, Tenable Network Security, Tripwire, and Qualys have extensive vulnerability libraries. Additionally, advanced malware sandbox platforms like Blue Coat Advanced Threat Protection, the FireEye Threat Management Platform, and Trend Micro ZDI Deep Discovery/TippingPoint Advanced Threat Protection make extensive use of vulnerability data.
- However, in large network security platforms, vulnerabilities are simply a factor to be considered in larger threat detection that also includes behavioral analysis, log correlation, and the chaining of events to uncover the existence of zero-day vulnerabilities. .
- While the number of companies offering a public disclosure program is diminishing; so to is the idea of individual companies disclosing breaches.
- In the Symantec Internet Security Threat Report (ISTR), Symantec reports, “Companies choosing not to report the number of records lost increased by 85%”.
- This raises two countervailing concerns. Naturally individual companies may be reticent to disclose breaches for fear that they are still vulnerable, may create an indemnity, and frankly believe that any public disclosure shows incompetency.
- However, the greater security community requires transparency which is the long card of global network security. The collection of vulnerability data is an integral process in the fine-tuning of cyber security appliances and platforms.
- The very formal platforms presented by Trend Micro’s Zero Day Initiative and Google’s Project Zero seem to be relics of an era when cyber security companies reported vulnerabilities to both enlighten their own communities, but also to prove the excellence of their own platforms.

Source: Frost & Sullivan analysis.

The Status of Public Vulnerability Reporting—Then, Now, and in the Future (continued)

- Some of these practices are naturally subsumed by other crowdsourcing and threat grid initiatives.
- Cisco Threat Grid and Open Threat Exchange (OTX) sponsored by Alien Vault are examples of privately supported, but available-to-the-public threat grid exchanges. (The advantage of these private threat grids is when any appliance under these companies' threat management network detected malware, the information is shared with all of the appliances on the network).
- As mentioned earlier in the report, the STIX/TAXII information sharing structure has great potential to not only unify B2B security platforms, but can be implemented as a protective fabric to include governmental threat data collection (to the degree potential participants share).
- Frost & Sullivan is an advocate of private bug bounty programs and see the necessity for individual companies to solicit the input of the individual contributor and there is still a role for ethical hackers.
- The end goal for security practitioners and the network administrators remains the same. The line of communications from the security platforms that find threat information has to result in successful patching.
- With this as the barometer, the relationships between PSIRT teams and security appliance teams continues has never been better.
- Using a hypothetical, if FireEye discovers a vulnerability with a General Motors application, the odds of getting detailed information about the threat conditions to Bank of America are better in 2016 then in 2015 (and quantitatively better than in 2010-11).
- Still, Frost & Sullivan found 1,337 vulnerabilities that were reported in great detail over public vulnerability disclosure Websites. These included high value vulnerability detection in highly used and high value assets like Adobe Flash, Internet Explorer and various mobile OS.
- Public vulnerability disclosure remains a vital part of the network security landscape.

Source: Frost & Sullivan analysis.

Profiles of Security Platform Providers Offering Public Vulnerability Disclosure

Core Security

- Core Security, the result of Courion's December 2015 acquisition of Core Security, is focused on providing enterprises with threat-aware, identity, access and vulnerability management solutions.
- Identifying and analyzing vulnerabilities are a principal area of the acquired Core Security with advisories on vulnerabilities published in CoreLabs Information Security Advisories: https://www.coresecurity.com/grid/advisories.
- The company's products span: identity and access management, vulnerability management, and network detection and response. While all three leverage vulnerability analysis, the vulnerability management product line is most closely aligned with use of software vulnerabilities.
- Core Security's vulnerability management product line consists of these two products:
  - Core Impact - Provides customized assessment and testing of security vulnerabilities, featuring:
    - Multi-vector testing across network, Web, and mobile
    - Penetration testing equipped with a comprehensive, real-time library of CVEs
    - Confirmation that remediation of identified vulnerabilities has been accomplished
    - Controlled client-side exploit testing
  - Core Vulnerability Insight (formerly Core Insight) – Unifies, regulates, and prioritizes vulnerability management initiatives enterprise-wide, featuring:
    - Consolidation and prioritization of vulnerabilities
    - Configurable threat modelling scenarios
    - Identification and elimination of attack paths to critical assets
    - Flexible reporting

Source: Frost & Sullivan analysis.

FortiGuard Labs (Fortinet)

- Fortinet is one of the largest pure-play network security companies in the industry. The company is best known for its FortiGate line of firewall appliances capable of performing a range of security functions such as NGFW (application visibility and control, user identity aware controls, IPS, and stateful firewall), gateway AV, email security, and Web filtering.
- Fortinet has a patent for Compact Pattern Recognition Language (CPRL) which does an emulation of malware. The purpose of CPRL is to use AV not only for the detection of malware, but also to detect Advanced Persistent Threats.
- Fortinet is now a $1 billion company and employees more than 4,500 people.
- Fortinet is the company name, but the company engine is FortiGuard Labs.
- FortiGuard Labs has several important functions:
  - FortiGuard Labs is responsible for turning bidirectional data from the installed base of Fortinet sensors and appliances into actionable data.
  - Fortinet is a member of the Cyber Threat Alliance. FortiGuard Labs most reign in the massive amount of data from its own appliances and sensors with what is learned through the Cyber Threat Alliance to uncover various types of attacks including advanced persistent threats.
  - FortiGuard Labs also pushes security updates to Fortinet clients; there can be as many as six updates in a day.
- The depth of information Fortinet produces in its annual threat report is impressive—coverage areas include malware, mobile malware, botnets, Web, spam, network vulnerabilities and zero-day threats.

Source: Frost & Sullivan analysis.

Google Project Zero (Google)

- Google is something of an outlier in this study. Unlike Trend Micro ZDI, High-Tech Bridge, and other companies that offer cyber security products, for all intent and purposes, Google is not a cyber security company in the conventional sense.
- However it is likely no company is more leveraged or has a more vested interest in the health of the Internet than Google.
- Google now owns eight platforms that have more than **1 billion** end users: Gmail, You Tube, Google Play, Google Chrome, Google Search, Android, Google Maps, and Google Drive.
- To Google's greater credit, the company develops applications and services (almost exclusively) on open platforms. The openness allows other technology companies to build dedicated connectors and APIs extending the reach and capability of programs.
- According to Statista: Google advertising and ad revenue, advertising represented $67.4 billion of revenue for Google in 2015.
- The keyword search is the strongest segment of the Google advertising spend.
- In a Official Google Webmaster Central Blog: HTTPS as a ranking signal, and in wider implementation in September 2014, Google made Web security a metric in keyword searches.
- The Google metric favors Websites with universal Hypertext Transfer Protocol Secure (HTTPS) protection and sites using 2048-bit SSL/TLS certificates. Additionally, Websites and that ensured that the relative Uniform Resource Locator (URLs) for resources resided on the same secure domain would also receive a preferential ranking if other factors were equal.
- Google Cloud is in active competition with Amazon Web Services and Microsoft Azure for cloud hosting services.
- Google has decided to compete by offering superior execution in Tensorflow machine learning and libraries, BigQuery monitoring, Kubernetes orchestration, and flat rate pricing—Internet hygiene will be an important component of Google's cloud success moving forward.

Source: Frost & Sullivan analysis.

Google Project Zero (Google) (continued)

About Google Project Zero

- The formation of Google Project Zero was announced by Google as a way to disclose software vulnerabilities that were likely to be used by Google end users.
- On July 14, 2015, Google announced the public existence of Google Project Zero.
- Upon its inception, Google Project Zero was met with mixed criticisms. Google Project Zero was lauded because any disclosure program creates an incentive for vendors with bugs or vulnerabilities in their software to patch the defect as quickly as possible.
- However, some companies expressed concern. Google Project Zero made a firm commitment to give vendors 90 days (after notification) to fix the vulnerabilities. On the 91st day, Google Project Zero would begin to publish pieces of the vulnerable code.
- Perhaps inevitably, Google Project Zero had a “bug” in its bug reporting platform. In February 2015, Google Project Zero revealed some of the exploitable code to Windows 8—even as Microsoft indicated to Google that a patch was forthcoming.
- Google revised its disclosure policy after the incident to allow an extension of 14 business days before disclosure provided that the affected vendor notifies Google that a patch will be released.
- Along with the extended grace period, Google also created a CVE identifier which enables others sources the ability to study vulnerabilities independently.
- On the following page, a screen capture shows details about an incident that has been reported and is now fixed.
- Each Issue in Project Zero has a finder, assigns a project owner, a report date, a CVE number, and posts an established deadline.
- Collaborators can rate the accuracy of the reporting and import notes/findings of their own.

Source: Frost & Sullivan analysis.

Google Project Zero (Google) (continued)

☆ Issue 467
Starred by 2 users

Status: Fixed
Owner: candrian@google.com
Closed: Sep 2015
Cc: project-...@google.com
Finder-candrian
Product-qlmanage
Severity-Medium
CVE-2015-3783
Deadline-90
Reported-2015-Jun-26
Vendor-Apple
CCProjectZeroMembers

Add a comment below

Apple qlmanage - heap overflow in SceneKit::daeElement::setElementName
Reported by candrian@google.com, Jun 26 2015

Back to list

```
There is a heap overflow in daeElement::setElementName(). The
vulnerable method uses a fixed size (128 bytes) heap-allocated buffer to
copy the name of an arbitrary element. By setting the name of the element
to something larger the buffer is overflown.

The vulnerable code does something like this:
if (element_name) {
  if (!this->name) {
    this->name = new char[128];
  }
  strcpy(this->name, element_name);
}

The element_name is supplied by the user and can be more than 128
characters long.

Steps to reproduce (Note: you need to enable libgmalloc):
a) $ lldb
b) (lldb) target create /usr/bin/qlmanage
   Current executable set to '/usr/bin/qlmanage' (x86_64).
c) (lldb) env DYLD_INSERT_LIBRARIES=/usr/lib/libgmalloc.dylib
d) (lldb) process launch -- -p setElementNameOOB.dae
    Process 4460 stopped
    * thread #3: tid = 0x5fdc, 0x00007fff92fbf108 libsystem_c.dylib`strcpy + 104, queue = 'com.apple.root.default-qos', stop reason
```

About Google Project Zero (continued)

- Each issue can be filtered to query different vulnerability statuses, the filter categories include: fixed, duplicate, invalid, wont fix. An “open issues” radio dial shows incidents that have not been fully investigated.
- Google Project Zero supplements its Project Zero reporting with blogs and extended analysis.
- Google has been active in the bug bounty rewards system.
- Perhaps no company is as circumspect about its own products. The Google Security Rewards Program includes Google Vulnerability Reward Program (VRP), Patch Reward Program, Vulnerability Research Grants, Chrome Reward Program, and the Android Reward Program.
- In a June 2016 article in Digital Trends Online Magazine, Google said it paid $550,000 through its Android Security Rewards Program, and has paid over $1 million in bounties over all Google platforms.

Source: Frost & Sullivan analysis.

High-Tech Bridge

- High-Tech Bridge is a specialist in penetration testing services (also known as ethical hacking), primarily offered through its ImmuniWeb Web application testing platform.
- The ImmuniWeb application testing platform represents a unique blend of manual penetration testing techniques and proprietary vulnerability assessment technologies. High-Tech Bridge utilizes machine learning to identify new vulnerabilities that are missed by traditional analysis techniques.
- High-Tech Bridge also offers free SSL server security testing, Web server testing, malicious domain discovery services, and regulatory compliance testing.
- For High-Tech Bridge, vulnerability research is “part of the territory.”
- High-Tech Bridge conducts security research testing in order to hone its ethical hacking skills. Vulnerabilities can also be uncovered by High-Tech Bridge through the process of testing for weak points in a client’s IT infrastructure.
- Since the announcement of its formal research program, the company has made a quantifiable impact on the security industry. High-Tech Bridge has released over 500 advisories, collaborating with hundreds of software vendors to fix over 1,000 unique vulnerabilities.
- In addition to original vulnerability research, High-Tech Bridge publishes regular reports on Web security trends and articles on emerging threats.

Source: Frost & Sullivan analysis.

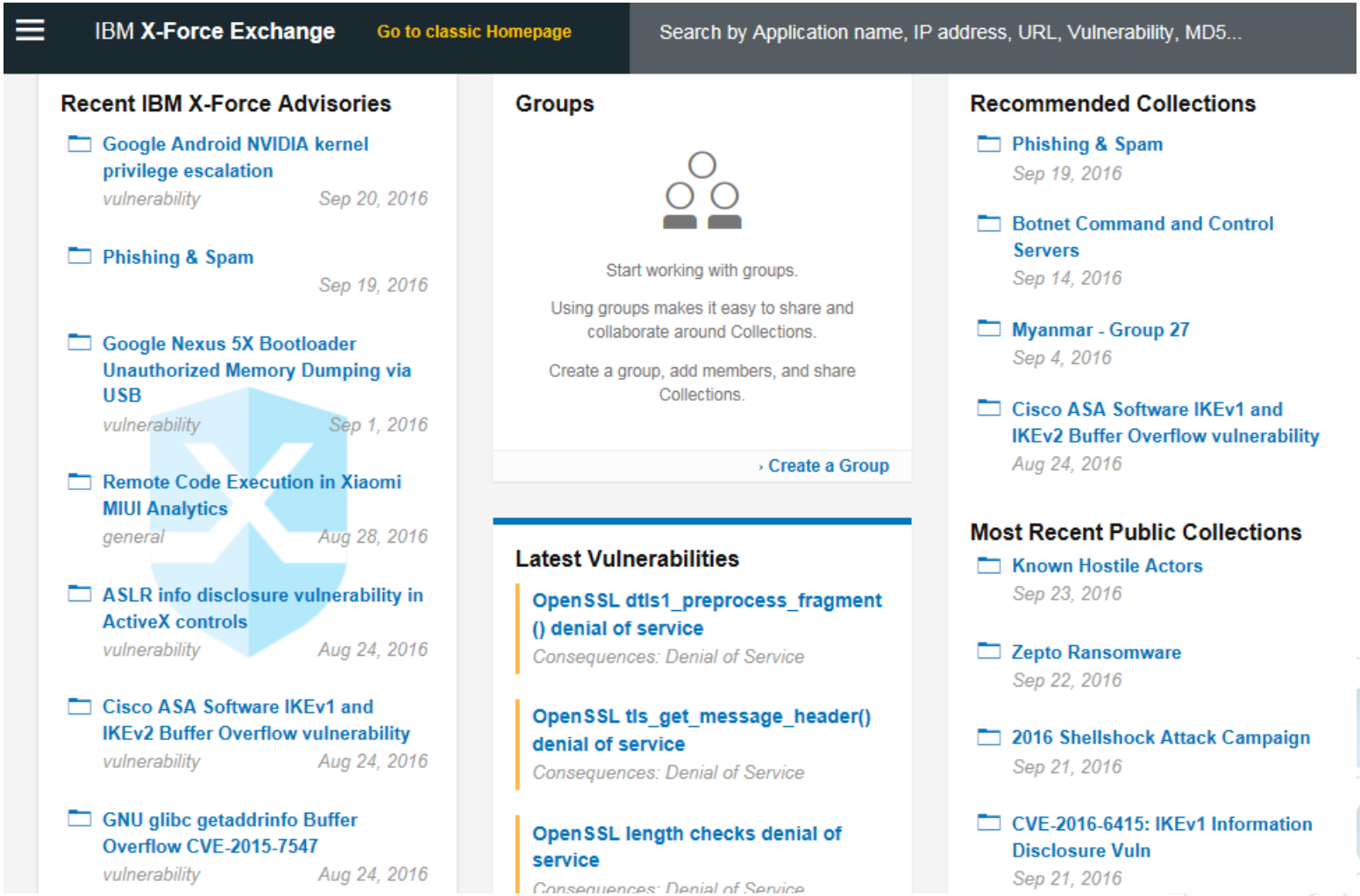
IBM X-Force (IBM)

- Between 2014 and 2015, IBM X-Force dramatically changed the way its public vulnerabilities were reported. The filters for granular investigation have been dramatically improved to weave in the number of malicious IP addresses discovered within the last hour, groups created via crowdsourcing, recommended collections, and IBM Security blogs (see screen capture on the next page).
- The most significant change in this publicly available platform is the depth of reporting. Instead of publishing public advisories about vulnerabilities (CVE numbers), the IBM X-Force Exchange includes information about:
  - **- MAL.** The types of malware detected.
  - **- URL.** Includes Websites, computer hardware.
  - **- MWF.** Links to information about large malware families.
  - *** - IP.** IP Addresses determined to be malicious.
  - *** - FILE.** Reports which files are considered vulnerable.
  - * **- VUL.** Represents traditional CVSS scoring metrics.

- The degree that end users can interact with IBM X-Force Exchange is impressive. The public reporting is helpful, but end users can also set up their own groups (often used by companies in specific vertical industries such as healthcare and financial sectors).
- The filters create hierarchies that be chained back into a report or a reporting mechanism designed for added input. Another SOC analyst can image other pieces of code that match threat data consistent with other pieces of the kill chain (malware family, effected IP/URL, etc.)

Source: Frost & Sullivan analysis.

IBM X-Force (IBM) (continued)



IBM X-Force Exchange Web Page Capture 09/26/2016

Source: Frost & Sullivan analysis.

IBM X-Force (IBM) (continued)

How IBM uses X-Force Exchange Data

- One of the prevailing themes in network security is that no one technology, or even one set of related technologies, guarantees a perfect network security posture. Frost & Sullivan sees the necessity and gained insight between discrete security technologies communicating bidirectionally for added visibility and added network control.
- However, only a few companies with a global presence can “shoot the moon.” Cisco, HP, and IBM have nearly comprehensive endpoint-to-core-thru-cloud network security technologies.
- IBM QRadar Security Analytics Platform is the ambitious, continually expanding network security platform offered by IBM.
- (From the IBM Website) IBM QRadar Security Intelligence Platform delivers:
  - A single architecture for analyzing log events, NetFlows, network packets, vulnerabilities, user and asset data.
  - Real-time correlation employing Sense Analytics to identify high-risk threats, attacks and security breaches.
  - Prioritization of high-priority incidents among billions of daily data points received.
  - Proactive analysis of existing risks due to device configurational issues and known vulnerabilities.
  - Automated incident response.
  - Automated regulatory compliance with data collection, correlation and reporting capabilities.
- The X-Force Exchange data is used with data from the bidirectional input of various IBM appliances to sharpen IBM security tools.
- When software revisions are made to the IBM IDS/IPS, SIEM, or IBM Security AppScan, the collaboration of data from IBM appliances and X-Force Exchange is used.

Source: Frost & Sullivan analysis.

Secunia (now Flexera)

- In September 2015, Flexera announced plans to acquire Secunia, and ultimately the deal was completed in December 2015.
- The following profile is largely about Secunia Research as it relates to public vulnerabilities. However, a few insights could be gained about why Flexera acquired Secunia:
  - In an online story by AlphaGen - What does Secunia's acquisition by Flexera mean for you?, the article explains that at the heart of Flexera technologies was software asset management tools, and the essence of Secunia is its vulnerability and patch management capabilities.
  - The combined competencies give IT departments a contextual analysis of a threat environment taking in asset and inventory management as a factor in determining which threats to address.
  - Existing Flexera technology gives greater depth at the application level for Secunia vulnerability and patch management platforms.
- Legacy Secunia products have been rebranded as Flexera. For the year 2015, the Secunia name was attached to the products and will be used that way in the report.
- While Flexera offers application inventory, management, readiness, virtualization, and workflow tools, Secunia products include the Corporate Software Inspector, Vulnerability Intelligence Manager, and Personal Software Inspector.
- The larger purpose of Secunia Research has been to support these product lines.
- Perhaps the most notable product produced by Secunia is the Personal Software Inspector (PSI). Secunia PSI has an installed base of roughly nine million devices.
- When an end user (largely consumers) download PSI, Secunia gains knowledge about the applications on the computer.

Source: Frost & Sullivan analysis.

Secunia (now Flexera) (continued)

- According to the Vulnerability Review 2016 | Flexera Software, the average PC had 79 programs installed.
- The (now) Flexera annual report is extremely useful to the network security analytics community. The report shows vulnerability data about Microsoft applications, non-Microsoft applications, and OS. The most influential reporting comes from the Top 50 software portfolio. Key findings from the 2016 report (for the year 2015) include:
  - In regard to patching, Secunia found 83.6% of vulnerabilities in all products, and 84.6% of vulnerabilities in products in the Top 50 software portfolio have a patch available on the day of disclosure.
  - According to Secunia, 57.0% of all attacks were triggered from a remote network (down from 73.5% in 2013). The local network was the point of origin for 35.5% of attacks, and the local system accounted for the remaining 7.5% of attacks in 2015.
  - Secunia Research, found the absolute number of vulnerabilities detected was 16,081.
  - The Top 5 applications found on PCS by Secunia in 2015 were all Microsoft applications (Windows Script Controls, XML Core Security Services (MSXML). .NET Framework, Windows Media Player, and Internet Explorer). In terms of vulnerabilities, Google Chrome and Adobe Flash Player had the most vulnerabilities reported with 516 and 457 respectively.
- In August 2013, Secunia discontinued its Secunia Vulnerability Coordination Reward Program (SVCRP). The program was launched in November 2011.
- For all intent and purposes, the formal public vulnerability advisory program is moribund. In 2015, Secunia issued six Advisories entailing seven vulnerabilities.
- At its peak in 2011, Secunia issued 225 Advisories covering 435 vulnerabilities.

Source: Frost & Sullivan analysis.

Secunia Research About Often-Targeted Applications (Adobe, Flash, and Microsoft)

- In its annual survey, Secunia found that Microsoft applications represented 40% of all applications on a personal computer, but that percentage grows to 67% of the Top 50 applications stored on PCs.
- However, despite the presence of Microsoft in PC applications, it can be argued that its non-Microsoft applications that are most vulnerable. In 2015, Secunia found 79% of vulnerabilities affecting the Top 50 applications came from non-Microsoft applications.
- One of the neat things about the Secunia Personal Software Inspector is that it does not discern between OS. In April 2014, Microsoft put an end-of-life to support for Microsoft Windows XP. Secunia Research found that as of December 2015, 11.8% of all global end users *still* used Windows XP.
- According to Secunia Research, PDF readers were more buggy in 2015 than in 2014. In 2015, Secunia researchers uncovered 147 vulnerabilities as opposed to 45 vulnerabilities uncovered in 2014.
- Secunia found 133 vulnerabilities in Adobe Reader. The number of vulnerabilities is concerning, but in many ways the security concerns for personal PCs is more acute than the concerns for applications in corporate environments. Business environments often have a centralized mechanism to push patches to endpoints. In the scan data generated from Secunia PSI, 42% of Adobe Flash vulnerabilities were left unpatched in 2015. (Worth noting this unpatched percentage was higher for other PDF readers).

Source: Frost & Sullivan analysis.

TippingPoint Zero Day Initiative (Trend Micro)

- TippingPoint is a manufacturer of network security solutions. The company has a history as one of the original pioneers of the IPS market. Trend Micro acquired TippingPoint in March 2016.
- The TippingPoint research division, called Digital Vaccine Labs (DVLabs), specializes in enterprise security and advanced threat trends and is a strong addition to Trend Micro research capabilities.
- Among its many responsibilities, TippingPoint DVLabs also conducts original vulnerability testing of key enterprise software systems. By doing so, TippingPoint can find vulnerabilities latent in the IT systems of some of its largest enterprise customers.
- TippingPoint then works with vendors to provide comprehensive analysis on vulnerabilities, including any related issues, and to coordinate a public vulnerability disclosure date that allows ample time for software vendors to develop and implement a patch or workaround. This thorough, coordinated process represents a stellar example of “responsible vulnerability disclosure practices.”
- TippingPoint maintains the Zero Day Initiative (ZDI) program which provides third-party researchers with monetary rewards in exchange for responsible disclosing of newly discovered vulnerabilities to TippingPoint.
- Additionally, TippingPoint has hosted a number of public hacking competitions such as the annual CanSecWest Pwn2Own (pronounced “pone-to-own”) contest. This contest is responsible for uncovering cutting edge vulnerabilities in some of the most important and ubiquitous software used today such as Google Chrome, Apple Safari, Microsoft Edge, and Adobe software.
- For TippingPoint customers, little is expected to change. Rather, Trend Micro is expected to extend the security research efforts of TippingPoint DVLabs.

Source: Frost & Sullivan analysis.

Trend Micro—TippingPoint Zero Day Initiative

- Even in the world of public vulnerability research and reporting, the Zero Day Initiative is unique for the depth and quality of its research.
- TippingPoint created the Zero Day Initiative (ZDI) on July 25, 2005.
- The goals and expected outcomes for ZDI are the same in 2016 as they were at the inception of the program (from the Zero Day Initiative Website):
  - Extend our DVLabs research team by leveraging the methodologies, expertise, and time of others.
  - Encourage the reporting of zero day vulnerabilities responsibly to the affected vendors by financially rewarding researchers.
  - Protect TippingPoint customers while the affected vendor is working on a patch.
- Research results come from both internal lab findings as well from individual (external) contributors.
- The contribution from individual researchers might be the most interesting. The Zero Day Initiative (ZDI) still offers financial incentives to individual contributors.
- This aspect alone encourages a type of specialization. Particular researchers might have a true competency at detecting command line or SQL injections (SQLi), cross site scripting (XSS) vulnerabilities or memory corruption bugs like “use after free” memory exploits.
- The ZDI has a loyalty rewards program for contributors where bonuses and other incentives can be rewarded for consistent achievement.
- The results from DVLabs and from the fully vetted vulnerabilities reported by individual contributors are used in TippingPoint's Digital Vaccine service and are being added to Trend Micro's Smart Protection Network.

Source: Frost & Sullivan analysis.

US-CERT

- Initiated in 2003, The United States Computer Emergency Readiness Team (US-CERT) is a branch of the Office of Cybersecurity and Communications' (CS&C) National Cybersecurity and Communications Integration Center (NCCIC).

- The US-CERT produces the National Vulnerability Database; which is what was used to normalize data published in this report.

- The US-CERT serves a different function than the more notorious National Security Agency (NSA). The US-CERT focuses on the preparedness of the US cyber defense program.

- A key part of that initiative is to coordinate the communication between commercial entities and the US government. The coordination effort has five broad objectives: communications, digital forensics, operations, international partnerships, and threat analysis and information sharing,

Source: Frost & Sullivan analysis.

Verisign (Verisign Labs)

- Verisign offers domain naming services (DNS) to private enterprises and to governments.
- Verisign gained its prominence in 2000, when it acquired Network Solutions which had transactional authority to issue domain names in conjunction with the Internet Corporation for Assigned Names and Numbers (ICANN) and the United States Department of Commerce.
- In 2014, the US government announced that it would no longer offer oversight of the domain-naming system. The announcement affected Verisign's share price.
- However, Verisign has a significant business in Web security offering security products for DDoS protection, DNS firewall, iDefense security intelligence, managed and recursive DNS.
- The bulk work of this report is about vulnerabilities determined through the CVSS v.2 scoring system which uses scan technology to find out where there may be configuration errors on endpoints. Self-evidently, network security also includes concerns about data, software authenticity, etc. Verisign Labs studies threat data that may effect the security involving DNS.
- Verisign Labs publishes results from threat data that it collects, but as importantly, Verisign Labs supports its customers and the larger security community through white papers, Webinars, and panels. Recent support activities include presentations titled:
  - Multi-Vantage Point Domain Name System (DNS) Diagnostics and Measurement. USTelecom Webinar
  - WHOIS No More: The Future of Registration Metadata
  - Domain Knowledge: How to Factor DNS into Your Privacy and Security Strategy. RSA Conference 2016

Source: Frost & Sullivan analysis.

Conclusions

Conclusions

1	Public vulnerability (PV) reporting is in a strange state. The idea of publicly disclosed “bug bounty” programs is fading away (although private bug bounty programs are cropping up). However, PV publishing could help with the larger idea of crowdsourcing shared threat data.
2	For the companies that make extensive use of PV reporting, there is a delicate balance between publishing and notifying PSIRT teams of emerging threats without giving a strategic edge to hackers.
3	It is not just software programs or improperly configured endpoints that are being compromised—firmware, software kernels, and Web applications are all exploitable.

Source: Frost & Sullivan analysis.

Appendix

Vulnerability Database Sources (for 2015)

- Current Network Security Advisories | Core Security
- FortiGuard Security Advisories | FortiGuard.com
- Google Project Zero - Monorail
- High-Tech Bridge Security Advisories
- IBM X-Force Exchange
- Computer Security Research - Secunia
- TippingPoint Zero Day Initiative
- US CERT Vulnerability Notes
- Verisign - List Of Publicly Disclosed Vulnerability Reports

List of Publications Cited in This Report

- Akamai [State of the Internet] 4Q 2015
- Bugcrowd, The State of the Bug Bounty, June 2016
- Cisco 2016 Annual Security Report
- Flexera Software (Secunia Research) Vulnerability Review 2016
- Fortinet 2016 CTAP Threat Landscape Report
- HealthcareInfoSecurity ENews
- High-Tech Bridge Security Research Blog
- HPE Cyber Risk Report 2016
- IBM X-Force Threat Intelligence Report 2016
- Intel Threats Predictions 2016
- SC Magazine (Daily Magazine) – cited many times
- SecureWorks – Underground Hacker Markets (April 2016)
- Symantec Internet Security Threat Report 2016
- Verizon Data Breach Investigations Report 2016

Source: Frost & Sullivan

Legal Disclaimer

- Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

- For information regarding permission, write to:

  Frost & Sullivan

  331 E. Evelyn Ave. Suite 100
  Mountain View, CA 94041

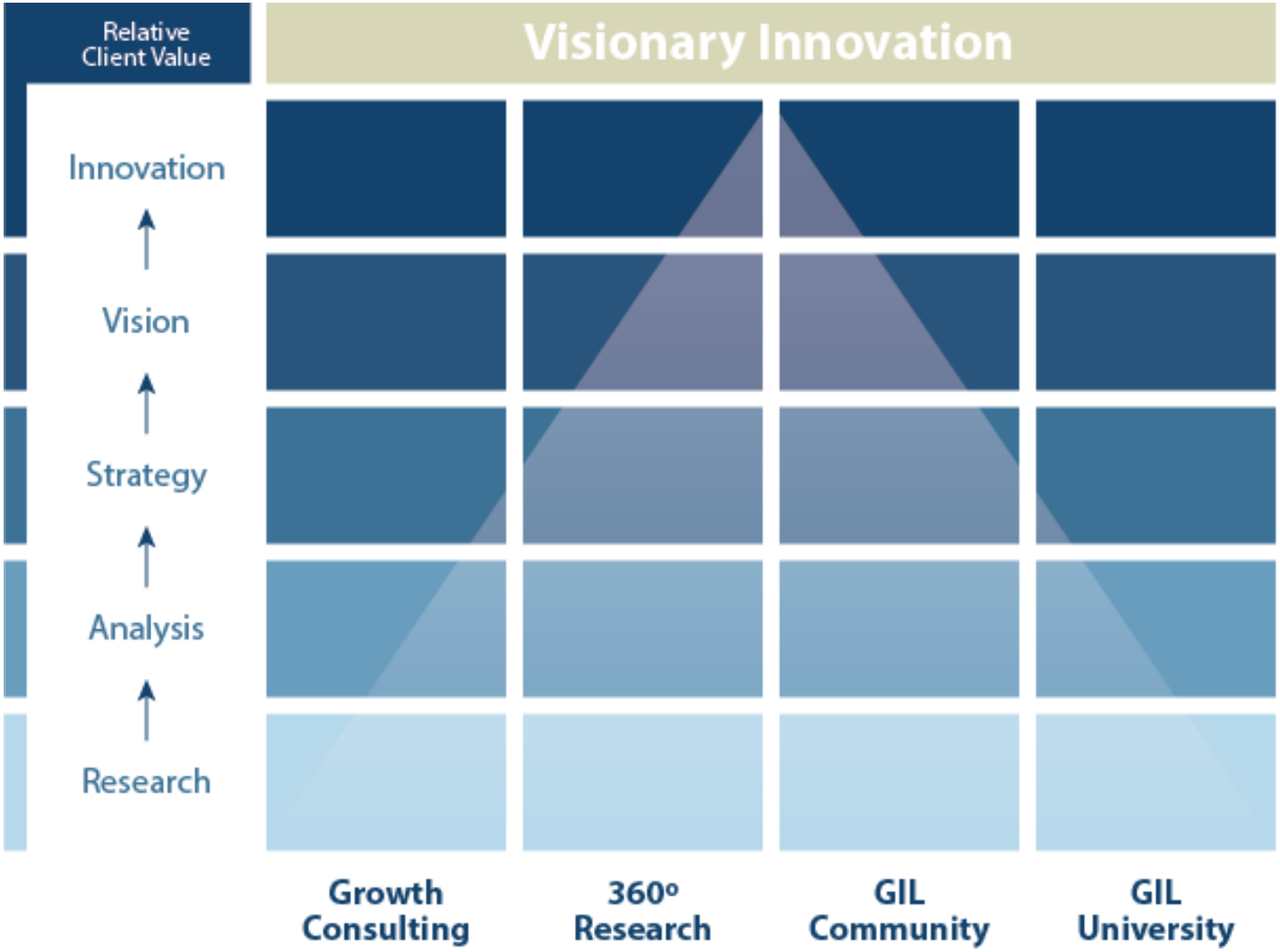
The Frost & Sullivan Story

The Journey to Visionary Innovation

The Frost & Sullivan Story

Value Proposition: Future of Your Company & Career

Our 4 Services Drive Each Level of Relative Client Value



Global Perspective

40+ Offices Monitoring for Opportunities and Challenges

Industry Convergence

Comprehensive Industry Coverage Sparks Innovation Opportunities

Aerospace & Defense

Measurement & Instrumentation

Consumer Technologies

Information & Communication Technologies

Automotive Transportation & Logistics

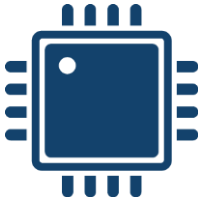
Energy & Power Systems

Environment & Building Technologies

Healthcare

Minerals & Mining

Chemicals, Materials & Food



Electronics & Security

Industrial Automation & Process Control

360º Research Perspective

Integration of 7 Research Methodologies Provides Visionary Perspective

Implementation Excellence

Leveraging Career Best Practices to Maximize Impact

Our Blue Ocean Strategy

Collaboration, Research and Vision Sparks Innovation