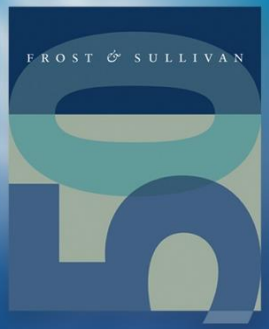
Analysis of the Global Public Vulnerability Research Market, 2017

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



February 2018

FROST & SULLIVAN

Research Team

Lead Analyst

Jason Reed
Industry Analyst
ICT – Digital Transformation

(647) 962-2944
Jason.Reed@Frost.com

Contributing Analyst

Chris Kissel
Industry Analyst
ICT – Network Security

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

Contributing Analyst

Tony Massimini
Industry Analyst
ICT – Network Security

(602) 301-7485
Tony.Massimini@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, FortiGuard Labs, Google Project Zero, Secunia Research, US-CERT, and Trend Micro Zero Day Initiative (ZDI).
  - 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 1,522 in 2017, an increase from the 1,262 in 2016, with the top three reporting agencies being:
  - Trend Micro ZDI had 1,009 verified, publicly reported vulnerabilities
  - Google Project Zero reported 340 vulnerabilities
  - US-CERT had 54 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 are 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), YARA, Structured Threat Information Expression (STIX), and Cyber Observable Expression (CybOX – which has now been integrated into 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. The Zero Day Initiative has held the Pwn2Own competition since 2007 (see next page).
- From 2010–2014, Google staged GooglePwnium contests. In 2016, Google scrapped the annual competition in preference to a year-round Chrome Vulnerability Reward Program. By January 2017, Google had paid $3 million in bug bounty rewards, one third of the total $9 million allocated to the program by the company.
- 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 2017 – Bugcrowd report (a few key findings below):
  - Bugcrowd has tracked more than 600 total programs, and of these, 77% were private programs and the remainder were public. Interestingly, it was not just programmers, software providers, or OS providers that offered bug bounties.
  - Bugcrowd reports there have been a total of $6.3 Million paid out across 96,000 total submissions.
  - The average payout per submission increased from $295 in the 2016 State of the Bug Bounty report, to $451 in the 2017 report, a 53% increase.

Source: Frost & Sullivan analysis.

Pwn2Own

- An important technical and cultural offspring of Trend Micro's Zero Day Initiative is the Pwn2Own contest sponsored by Trend Micro.
- 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.
- The technical details of the 'pwn' are provided to the affected vendor during the competition. They are then able to immediately start work on a security patch.
- The 2017 Pwn2Own competition saw $833,000 in prizes handed out.
- The 2017 Mobile Pwn2Own saw $515,000 in prizes handed out.

Source: Frost & Sullivan analysis.

Pwn2Own Competition

Year	Prizes Awarded	Biggest Prize Winner	Discoveries
2007	$10,000	Dino Dal Zovl	Dal Zovl and Shane MacAuley discover vulnerabilities in QuickTime (Safari).
2008	$10,000	Charlie Miller, Jake Honoroff and Mark Daniel of Independent Security Evaluators	Charlie Miller was able to a laptop running OSx using a bug found in Safari.
2009	$10,000	Within minutes of the contest opening, Charlie Miller hacked into MacBook, exploiting Safari on Osx without the aid of any browser plugins	The browser targets were Internet Explorer 8, Firefox, and Chrome installed on a Sony Vaio running Windows 7 Beta and Safari and Firefox installed on a MacBook running Mac OS X.
2010	$60,000	Based on the schedule of awards, Charlie Miller and Ralf-Philip Weinmann / Vincenzo Incenzo Iozzo won $15,000 apiece	The available cash pool climbed to a possible $40,000 for hacks to web browsers, and $50,000 for mobile phones.
2011	$30,000	VUPEN won $15,000 for Apple Safari Browser hack	By the end of the contest, Apple Safari, Internet Explorer, iPhone 4, and Blackberry Torch 9800 were exploited.
2012	$90,000	VUPEN was the top scorer and won $250,000	VUPEN was able to pwn Internet Explorer 9, Google Chrome, and Apple Safari. Significantly, Google felt there was a credibility gap because contestants did not need to disclose the full exploit.
2013	$480,000	VUPEN won $250,000	Vulnerabilities that were successfully presented at 2013 Pwn2Own were: Java, Internet Explorer, Mozilla Firefox, Adobe Flash, Google Chrome and Adobe Reader.
2014	$850,000	VUPEN won $400,000 over two days	Vulnerabilities that were successfully presented at 2014 Pwn2Own targeted Mozilla Firefox, Adobe Flash, Adobe Reader, Internet Explorer, Google Chrome, and Apple Safari. .
2016	$557,500	JungHoon Lee (aka Iokiheardt) won $225,000	The vulnerabilities discovered at 2016 Pwn2Own were: Microsoft Windows: 5, Internet Explorer 11: 4, Mozilla Firefox: 3, Adobe Reader: 3, Adobe Flash: 3, Apple Safari: 2, Google Chrome: 1.
2016	$460,000	Tencent Security Team Sniper (Kee nlab + PC Manager) won $142,500 and was declared Master of Pwn	The vulnerabilities discovered at 2016 Pwn2Own were: Microsoft Windows: 6, Apple OS X: 5, Adobe Flash: 4, Apple Safari: 3, Microsoft Edge: 2, Google Chrome: 1
2017	$833,000	360 Security	51 bugs were discovered and shared privately with vendors. Notably, Chrome browser was not exploited, making it the most secure browser, while Edge was exploited numerous times.

Source: Frost & Sullivan analysis.

Mobile Pwn2Own Competition

Year	Prizes Awarded	Biggest Prize Winner	Discoveries
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	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 exfiltrate cookies. Juri Aedia hacked Firefox.
2016	$215,000	Tencent Keen Security Lab Team	Mobile devices exploited 2016 in the Mobile Pwn2Own included Google Nexus 6P and iPhone 6S.
2017	$515,000	Tencent Keen Security Lab Team	A total of 32 unique bugs were submitted to the program over both days. Contestants were awarded $515,000 and multiple phones.

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 four primary types of CVE number assignments: Primary, Software Vendors, Third Party Coordinator, and Vulnerability Researcher.
  - The MITRE Corporation functions as editor and primary CNA.
  - Various CNAs assign CVE entries for their own products (i.e., Microsoft, HPE, Oracle, etc.).
  - Zero Day Initiative is able to assign CVE IDs as a third-party coordinator. 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.
- 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.
- 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.
- The formal reporting focuses on the base year 2017. In some cases, direct comparisons are made with 2016 publicly reported vulnerabilities.

Source: Frost & Sullivan analysis.

The Threat Environment in 2017 and Early 2018

The Threat Environment: Human Vulnerability

LACK OF AWARENESS AND INCOMPLETE TRAINING AMONG END-USERS CONTINUE TO POSE A MAJOR THREAT TO SECURITY.

- While hacking, DDoS, backdoors and exploits are prevalent, social engineering attacks are among the most common occurrences in today's threat landscape.
- In Verizon's 2017 Data Breach Investigation Report, the company reported that nearly half of all cyberattacks are socially engineered.
- End-users are often viewed as the weakest link in an organization's security apparatus, and as such are targeted directly by adversaries.
- Social engineering attacks are relatively homogenous in nature. Phishing and "pretexting" account for *"almost 98% of both incidents and breaches that involved a social action,"* according to Verizon.
  - Phishing and spearphishing are relatively well-known tactics employed by adversaries that usually take the form of an email that asks the user to download a file or click a link sent under the guise of a reliable source.
  - Pretexting, mostly the domain of organized crime, creates a scenario or a believable story that influences the end user to an action, such as transferring money from a corporate account to a supposed member.

The Threat Environment: Human Vulnerability

The Phishing Life Cycle

- Verizon identifies several stages in a successful phishing campaign.
  - Phishing to implant malware on the end user network.
  - Using stolen credentials as an entry point to the user's databases.
  - *"95% of phishing attacks that led to a breach were followed by some form of software installation."*
- The majority of phishing attacks are financially motivated, with the aim of monetizing the resulting breach.
- State actors also use this method to gain access to sensitive information.
- Phishing was particularly prolific in 2017, with Qatar, a nation of only 2.3 million inhabitants, subjected to more than 93,000 phishing events in Q1 of 2017, according to Kaspersky Labs.

The Threat Environment: Larger Organizations Are Targets

MAJOR ORGANIZATIONS ARE INCREASINGLY TARGETED, WITH POTENTIALLY DEVASTATING RESULTS.

- 2017 saw several high profile breaches, including two that are considered to be among the most significant breaches ever.

Equifax

- In July 2017, Equifax, one of the world's largest credit bureaus, suffered a data breach affecting 145 million people. Due to the scale of the breach, and the sensitivity of the stolen data, this hack was arguably the most impactful hack of 2017.
- Equifax CEO Richard Smith stepped down in the aftermath of the breach, and was called to testify in front of Congress. He blamed the security failure on a single individual who had since been removed from the company.

Yahoo

- Verizon, Yahoo's parent company, announced in October 2017 that each of Yahoo's 3 billion accounts had been compromised in prior years. This represents three times the number that was initially announced.
- The company still does not know who was responsible.

The Threat Environment: Chip Vulnerabilities

EARLY 2018 REVEALED MAJOR FLAWS IN CHIPS PRODUCED BY INTEL, AMD, AND OTHERS.

- Meltdown and Spectre, vulnerabilities that affect millions of devices, were revealed in January 2018. Chips from Intel, AMD, and ARM are vulnerable to the attacks. These chips are used in devices made by Apple, Google, Microsoft, and Amazon, among others.

Meltdown

- According to leading academics, *"Meltdown breaks all security assumptions given by address space isolation as well as paravirtualized environments and, thus, every security mechanism building upon this foundation. On affected systems, Meltdown enables an adversary to read memory of other processes or virtual machines in the cloud without any permissions or privileges, affecting millions of customers and virtually every user of a personal computer."*
- Not only does this vulnerability allow for the potential compromise of sensitive local data, it impacts cloud services as well as cloud hosting servers use the same chips. Furthermore, post-security update, Amazon AWS customers have noticed profoundly slower speeds and overall performance.

The Threat Environment: Chip Vulnerabilities

Spectre

- Academics note that *"Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre."*
- Spectre has proven harder to exploit than Meltdown, but it is also harder to mitigate or remediate.
- At the time of publication, no foolproof solutions for Spectre have been found.

The Threat Environment: Chip Vulnerabilities

MICROSOFT SMB EXPLOIT ETERNALBLUE, ORIGINALLY DESIGNED BY THE NSA, TURNED ON USERS FOR NEFARIOUS PURPOSES.

- Early in 2017, EternalBlue, an exploit developed by the NSA that was leaked by hacking group Shadow Brokers.
- EternalBlue is a software vulnerability in Microsoft's Windows operating system.
- The vulnerability exploits the Microsoft Server Message Block 1.0. The SMB is a network file sharing protocol.
- Soon after the leak by the Shadow Brokers, the exploit was used to launch the WannaCry ransomware attack that affected at least 230,000 computers across 150 countries. EternalBlue was then used to spearhead NotPetya.
- The exploit has emerged again in early 2018 in the form of WannaMine, which allows malware to tap into CPU power and use it to generate the digital currencies like Bitcoin and Monero.

Malicious Software: Malware

"Malware" refers to various forms of harmful software, such as viruses and ransomware. Once malware is in your computer, it can wreak all sorts of havoc, from taking control of your machine, to monitoring your actions and keystrokes, to silently sending all sorts of confidential data from your computer or network to the attacker's home base." – RAPID7

Some notable malware that caught our in 2017 attention include:

Universities and federal agencies targeted by malware

- A hacker known as Rasputin attacked more than 60 universities and US federal government organizations with SQL injections. Affected institutions include Oxford, Cambridge, and New York University, as well as the US National Oceanic and Atmospheric Administration.

Mac video encoder HandBrake infected with malware

- Thousands were at risk of infection with a remote access Trojan in early May 2017 when HandBrake, Apple's video encoder, was infected with malware. The malware could steal passwords from their Mac keychain.

Malicious Software: Malware

NotPetya

- The NotPetya virus encrypts the end user's files and data and shows a screen demanding a Bitcoin ransom to restore access. This upgraded version of the more benign Petya virus has some key defining characteristics that made it extremely dangerous. According to CSO Online:

"

  - *NotPetya spreads on its own. NotPetya exploits several different methods to spread without human intervention.*
  - *NotPetya encrypts everything. The NotPetya malware goes far beyond the original Petya trick of encrypting the master boot record, going after a number of other files.*
  - *NotPetya isn't ransomware. This is the most important thing about NotPetya. It looks like ransomware, complete with a screen informing the victim that they can decrypt their files if they send Bitcoin to a specified wallet. For Petya, this screen includes an identifying that they're supposed to send along with the ransom; the attackers use this code to figure out which victim just paid up. But on computers infected with NotPetya, this number is just randomly generated and would be of no help in identifying anything. And it turns out that in the process of encrypting the data, NotPetya damages it beyond repair.*

Malicious Software: Ransomware

In Verizon's 2017 Data Breach Investigation Report, the authors note that with the rise of Bitcoin and other anonymous payment systems, 2017 saw an explosion of the most sophisticated ransomware ever seen.

Some important ransomware events in 2017 and early 2018 include:

WannaCry

- Recognized as the largest ransomware attack yet, the WannaCry ransomware was successful thanks to the NSA losing control of its key hacking tools, EternalBlue. This SMB exploit allowed hackers to install backdoors that channeled the ransomware to hundreds of thousands of computers.
- Like most ransomware, the virus encrypted data and demanded Bitcoin payments to unlock the data.
- Mercifully, the attack was halted within days due to emergency patches released by Microsoft, and the discovery of a "kill switch" that stopped the spread of the ransomware.

Malicious Software: Ransomware

WannaMine (2018)

- New cryptocurrency mining viruses spread to Windows computers in early 2018.
- The viruses are spread using the EternalBlue exploit, which was used as part of the WannaCry ransomware attack.
- According to researchers from Proofpoint, a massive global botnet dubbed ‘Smominru’ is using EternalBlue SMB exploit to infect PCs and secretly mine monero cryptocurrency.
- Researchers believe that, at the time of publication, more than 526,000 computers have been infected.

Configuration Exploits: Botnets

Verizon's 2017 Data Breach Investigation Report found that a large number of breaches were the targets of botnet activity. Including botnets in their analysis, they found that 93% of breaches were associated with organized crime.

Notable botnet activity included:

WireX

- In August 2017, security researchers from several firms found a widespread botnet that consists of tens of thousands of hacked Android smartphones. Called WireX, the botnet network is designed to conduct enormous application layer DDoS attacks.
- Working together, the WireX botnet was taken down by a group of security firms.

Configuration Exploits: DDoS

Kaspersky Lab reports that cybercriminals increasingly used Distributed Denial of Service (DDoS) attacks in 2017, as 33% of organizations faced such an attack, up from 17% in 2016.

- Of those affected, 20% were very small businesses, 33% were SMBs, and 41% were enterprises.

One notable DDoS attack in 2017 was:

Dreamhost

- In August 2071, the web hosting organization DreamHost was attacked by a distributed denial of service attack, bringing down most of its services.
- The assault was notable because it was simultaneously blamed on extremists on both end of the political spectrum, for hosting far-left and far-right content.

Hardware Vulnerabilities: Internet of Things

In Cisco's 2017 Midyear Cybersecurity Report, researchers characterize the Internet of Things (IoT) as *"the inter-networking of physical devices, vehicles, buildings, and other items that are embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data."*

- As the IoT proliferates, so too do the security challenges associated with the connected devices. Security professionals, who often do have direct access to the devices in their network, struggle to keep pace with the threats emerging in the IoT field.
- In addition, Cisco notes, IoT devices typically:

"

  - *Have little or no CVE reporting or updating*
  - *Run on specialized architectures*
  - *Have unpatched or outdated applications that are vulnerable, like Windows XP*
  - *Are rarely patched*

Hardware Vulnerabilities: Internet of Things

- Attackers are increasingly targeting IoT-enabled networks in response to perceived weaknesses in their security architecture. In 2017, a survey conducted by Altman Vilandrie & Company found that nearly half of US businesses running IoT enabled devices had suffered an IoT-related security breach.
- If a more streamlined and codified approach to IoT security is not implemented in short order, IoT attacks are expected to continue to increase in frequency and intensity as more devices are connected.

As an example of IoT vulnerabilities, Trend Micro reported:

"The Mirai botnet attack is an example of how connected devices can be corrupted for ill purposes. In 2016, it managed to infect unsecure connected devices and use them to take down major websites such as Twitter and Netflix via massive distributed denial-of-service (DDoS) attacks. Variants of Mirai soon surfaced later in the year, including one that attacked 900,000 home routers provided by Deutsche Telekom. Within just a few hours on Nov. 29 last year, a new Mirai campaign detected in South American and North African countries was found to be responsible for 371,640 attack attempts coming from around 9,000 unique IP addresses."

Hardware Vulnerabilities: Point of Sale

Symantec reports that PoS data theft is one of the earliest forms of cybercrime and persists today. The note that *"point-of-sale malware is now one of the biggest sources of stolen payment cards for cybercriminals. Although it hit the headlines over the past year, the POS malware threat has been slowly germinating since 2005."*

Some notable PoS compromises in 2017 included:

- **Kmart** revealed that the store payment systems were infected with malware.
- **Forever 21** customers could have been affected by a potential data breach. Upon receiving a tip from a third-party, Forever 21 launched an investigation and found that some PoS devices were compromised.
- **Hyatt Hotels** discovered unauthorized access to its payment card information that were swiped at the front desks of some of its properties. Stolen information includes card numbers, expiration dates, internal verification codes, and cardholder names.

Hacking and Cyber-Espionage: 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.

Hacking and Cyber-Espionage: Advanced Persistent Threats (APT)

- 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.
- 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.

Insider Threats

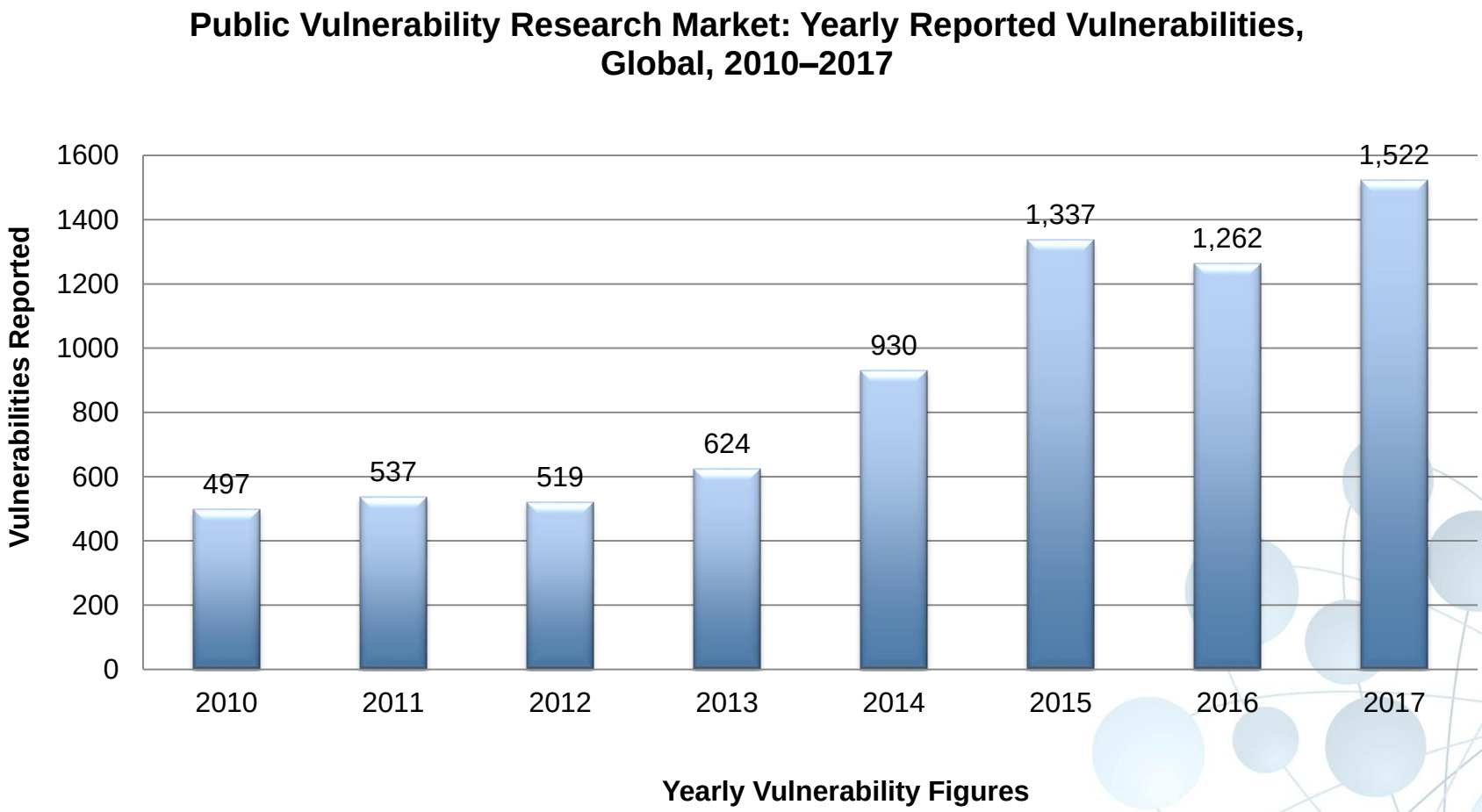
- Sometimes the greatest threats are from insiders with clearance to access secure information. One such example is the recent arrest of Jerry Chun Shing Lee, who is believed to have been a mole in the CIA that explained how the CIA was losing informants in China. As the New York Times reported:

"

- *Some intelligence officials believed that a mole inside the C.I.A. was exposing its roster of informants. Others thought that the Chinese government had hacked the C.I.A.'s covert communications used to talk to foreign sources of information.*
- *Still other former intelligence officials have also argued that the spy network might have been crippled by a combination of both, as well as sloppy tradecraft by agency officers in China. The counterintelligence investigation into how the Chinese managed to hunt down American agents was a source of friction between the C.I.A. and F.B.I.*

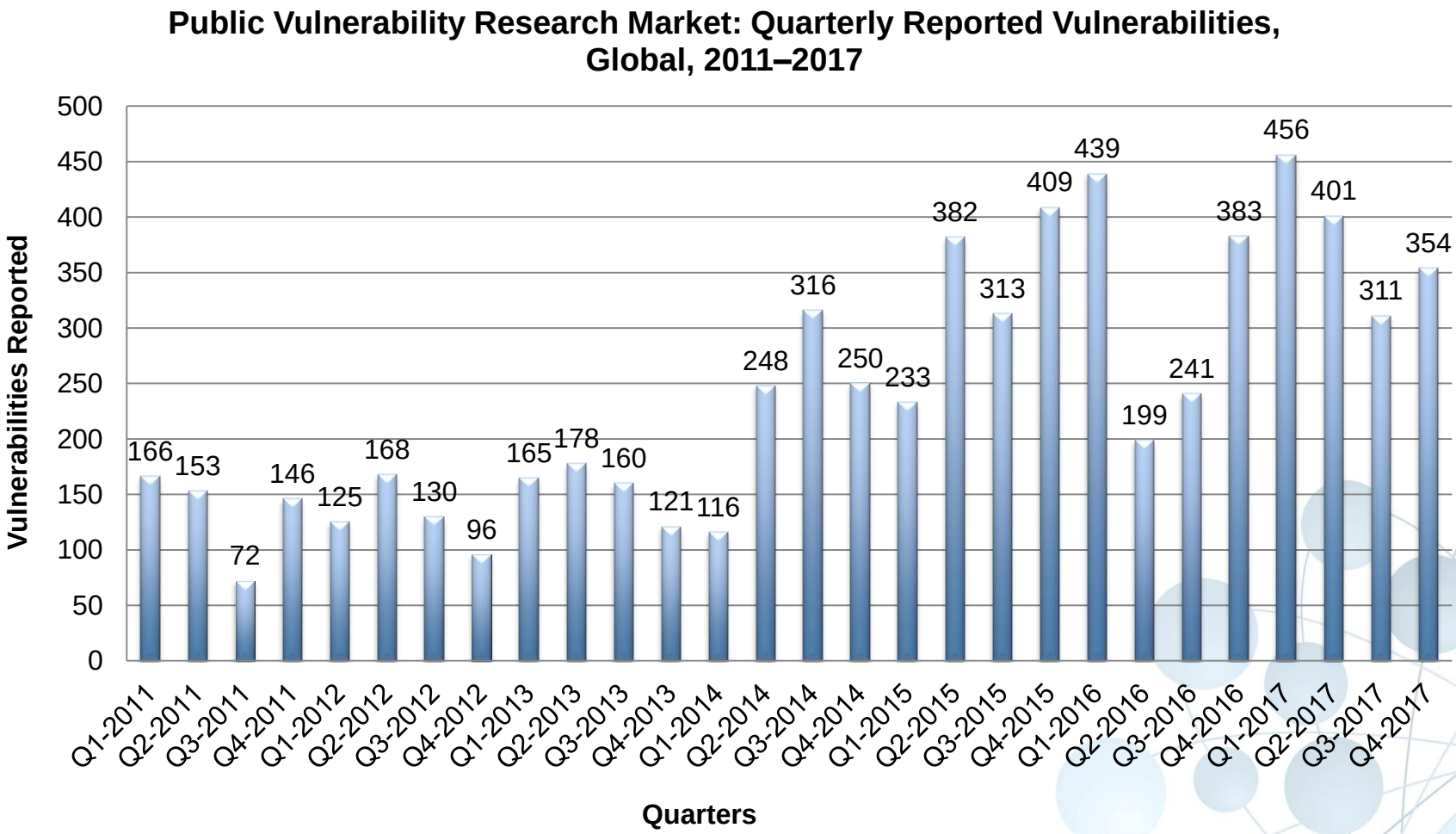
Market Trends in Public Vulnerabilities

Vulnerabilities Reported by Year



Note: All figures are rounded. Base year: 2017 Source: Frost & Sullivan analysis.

Quarterly Reported Vulnerabilities



N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017 Source: Frost & Sullivan analysis.

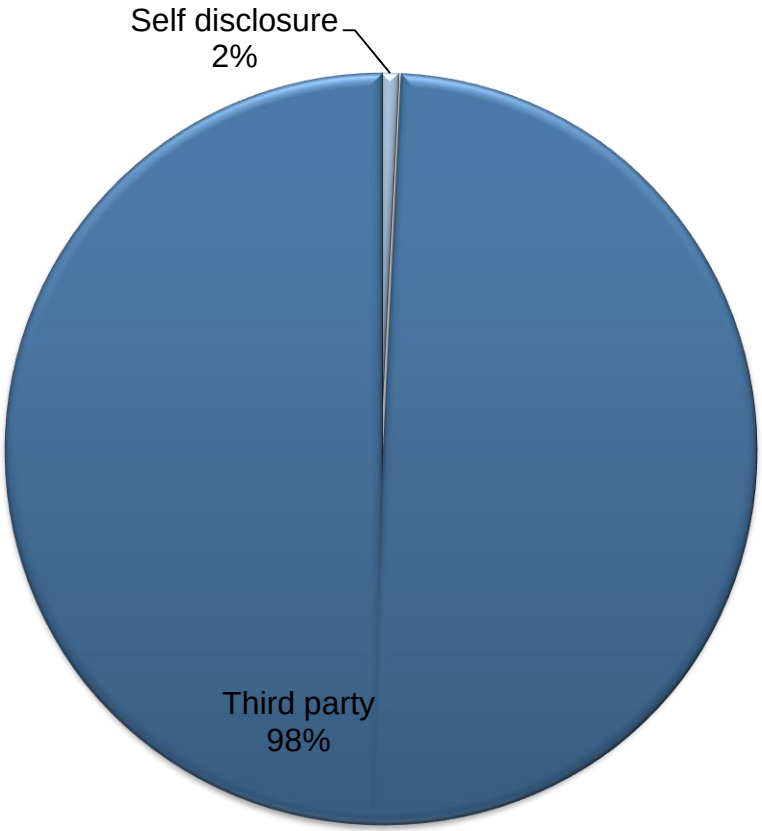
Market Trends

- Frost & Sullivan counts 1,522 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 in 2017 with 1,009, demonstrating the veracity of the Trend Micro contributor program.
- Trend Micro ZDI was the leading disclosing institution with 1,009 vulnerabilities in 2017, holding 66.3% share. This is a significant increase over 2016 with a gain of approximately 13 points.
- Google Project Zero has seen a decrease in reported vulnerabilities, down from 348 in 2016 to 340 in 2017. It holds 22.3% share of reported vulnerabilities, representing a loss of approximately 5 points since 2016.
- Overall, the total number of confirmed vulnerabilities increased substantially from 1,262 in 2016 to 1,522 in 2017. This was driven by a substantial increase in the number of vulnerabilities reported by Trend Micro ZDI.
- On a quarterly basis, more vulnerabilities appear to be reported in the first and last quarters. This could indicate a “summer slump” in vulnerability research.

Source: Frost & Sullivan analysis.

Vulnerability Disclosure

Public Vulnerability Research Market: Percentage of Reported Vulnerabilities by Disclosure Type Global, 2017



N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017 Source: Frost & Sullivan analysis.

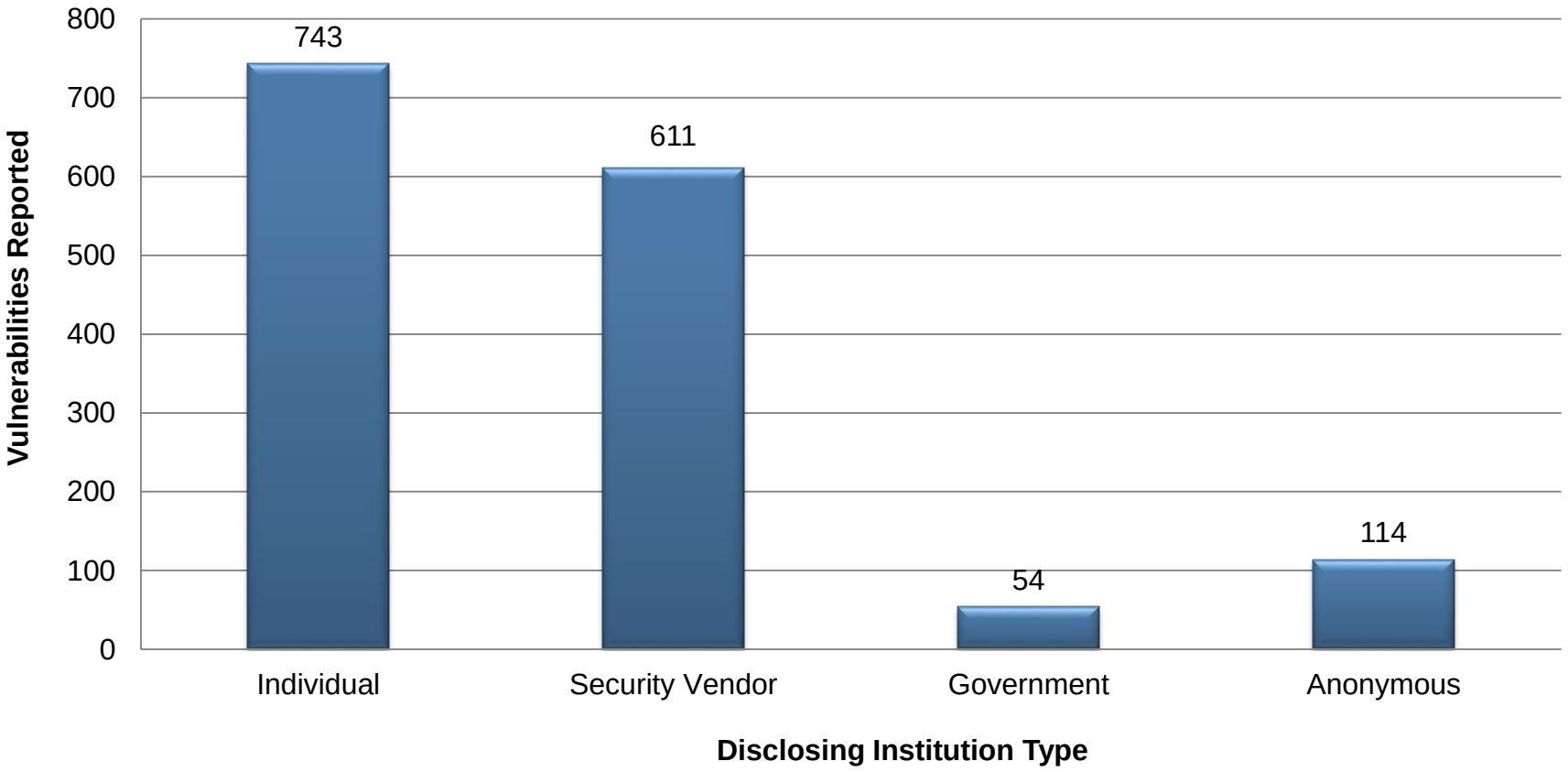
Vulnerability Disclosure (continued)

- 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 2017. Third-party sources discovered and reported 98% of vulnerabilities in 2017.
- Self-disclosed reports accounted for 2% of reported vulnerabilities.
- Manufacturers have different mechanisms for reporting vulnerabilities. Most companies issue advisories. Manufacturers such as 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 by Institution Type (continued)

Public Vulnerability Research Market: Reported Vulnerabilities by Organization Type Global, 2017



N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017 Source: Frost & Sullivan analysis.

Vulnerability Disclosure by Organization Type (continued)

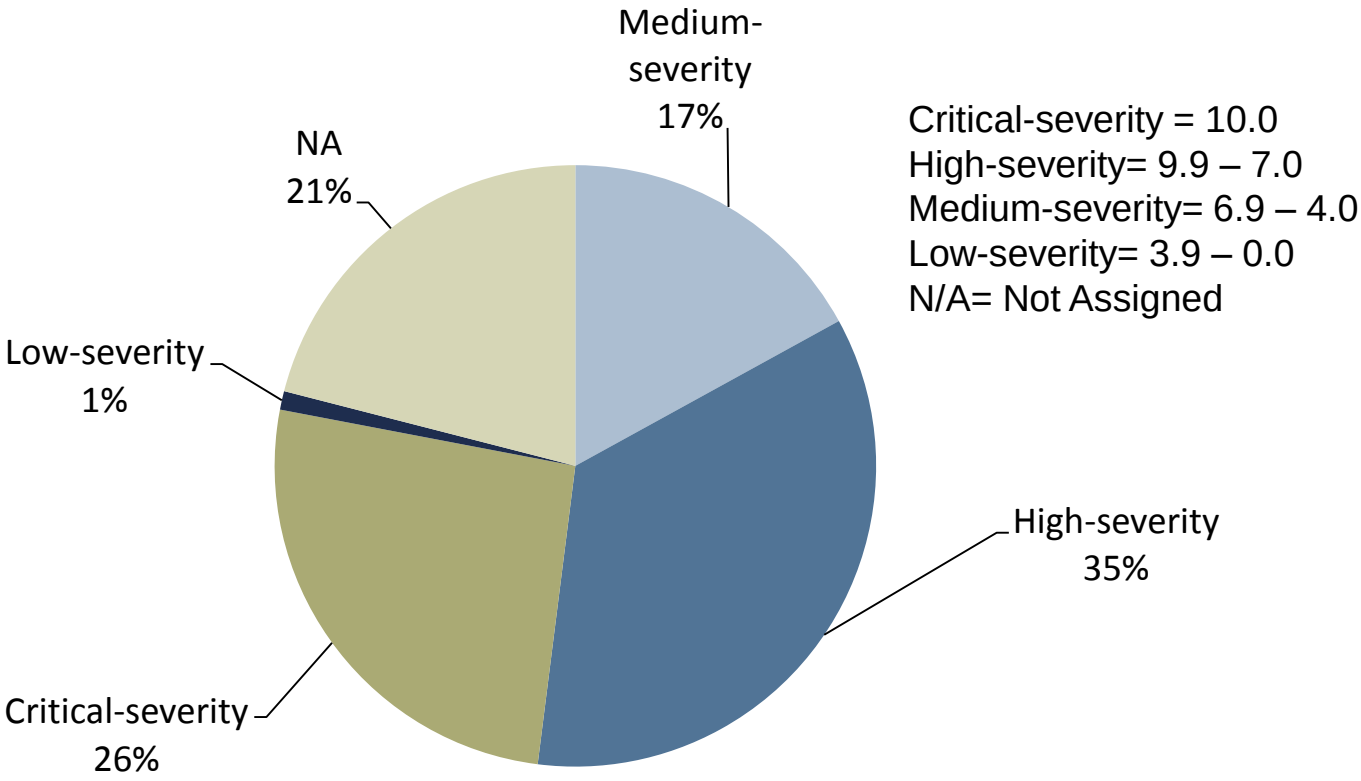
- Vulnerabilities disclosed by Trend Micro ZDI and Secunia were counted as individual if indicated in their disclosures. If the vulnerability was disclosed as Secunia Research, HPE ZDI (only prior to the Trend Micro acquisition of ZDI) or Trend Micro ZDI, it was counted in the Security vendor category.
- US-CERT vulnerabilities were counted with the Government category even if individually reported.
- In 2017, individual attribution of vulnerability discovery was 49%.
- Security vendors found 40% of all publicly disclosed vulnerabilities.
- Seven percent of vulnerabilities were anonymously disclosed or the attribution is unknown.
- Compared to 2016, the ratio of security vendors, individuals, and government disclosures remained fairly consistent, with minor but statistically insignificant changes.

Source: Frost & Sullivan analysis.

Analysis of Vulnerability by Severity

Analysis of Vulnerabilities by Severity

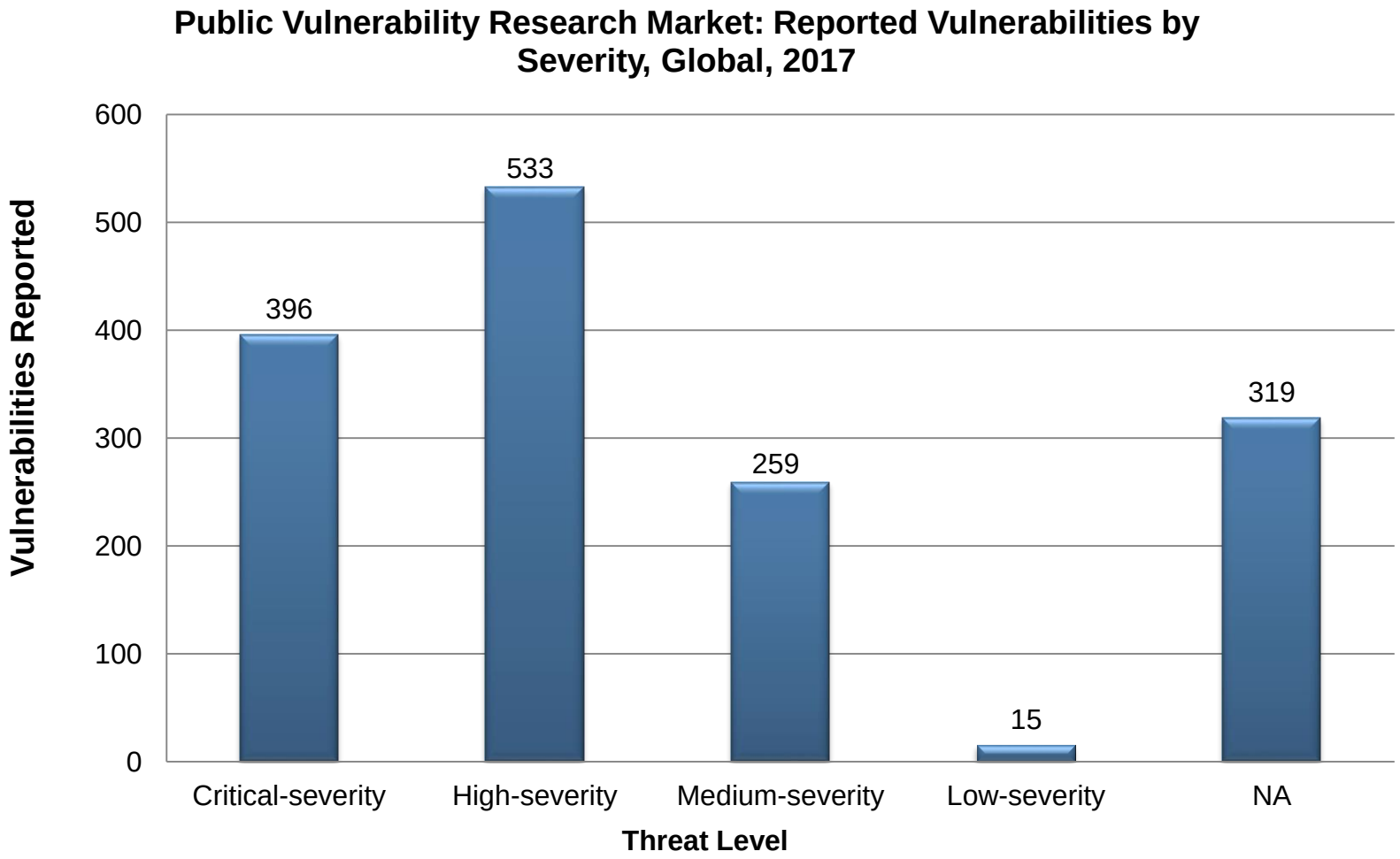
Public Vulnerability Research Market: Percentage of Reported Vulnerabilities by Severity, Global 2017



N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017 Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)



N=1,522 vulnerabilities

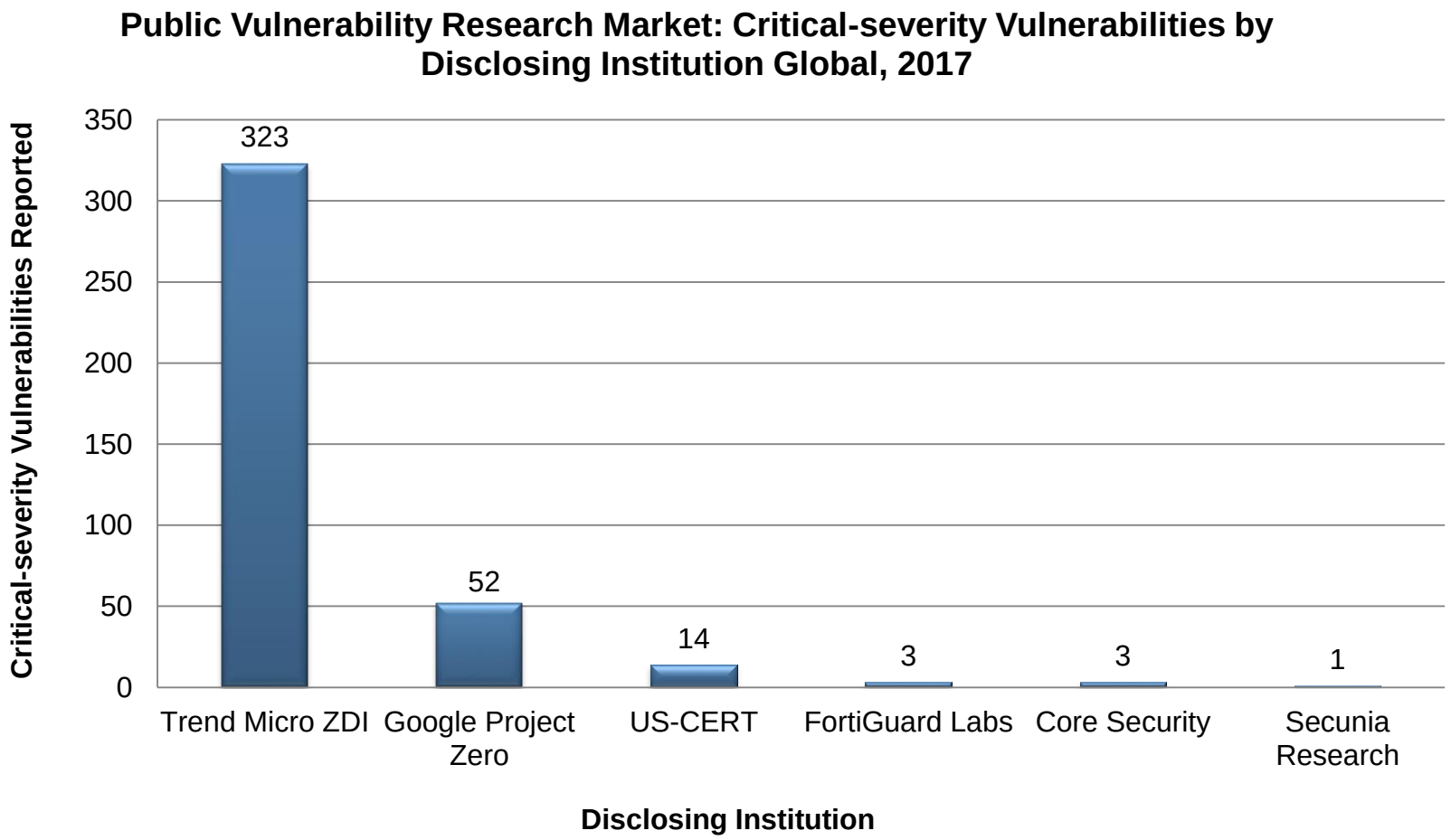
Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

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 2017, critical vulnerabilities rated 10.0 by the NVD amounted to 26% of vulnerabilities disclosed. This was grew slightly from the 23% share by the same disclosing institutions in 2016.
- 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 35% of disclosed vulnerabilities in 2017. This is down from 32% in 2016. 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 17% and 1% of vulnerabilities disclosed, respectively.
- Vulnerabilities which were unknown or not assigned a severity ranking, NA, decreased slightly from 27% in 2016 to 21% in 2017.

Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

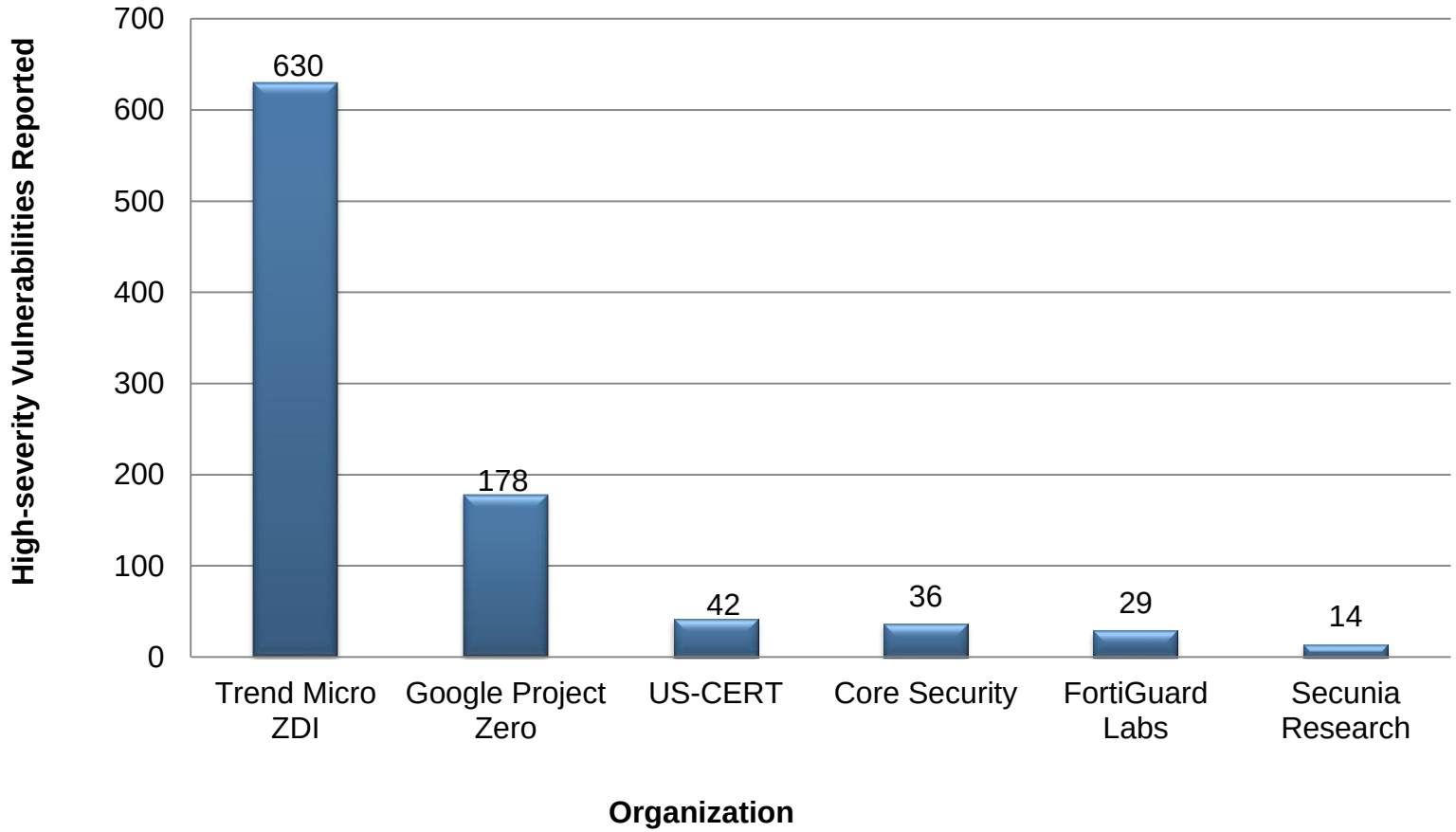


N=396 vulnerabilities

Note: All figures are rounded. The base year is 2017 Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

Public Vulnerability Research Market: Critical & High-severity Vulnerabilities by Reporting Source, Global, 2017



N=929 vulnerabilities

Note: All figures are rounded. The base year is 2017 Source: Frost & Sullivan analysis.

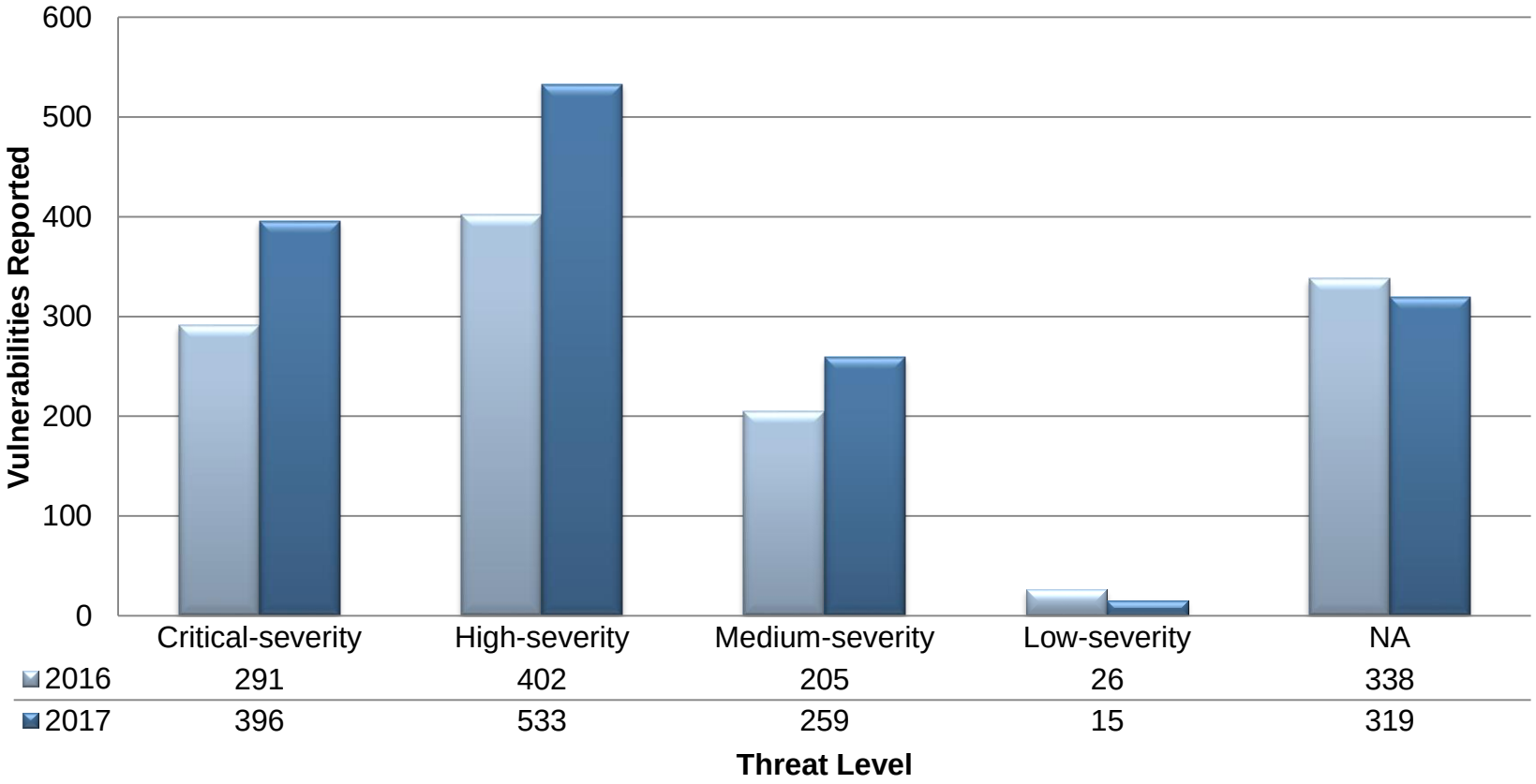
Analysis of Vulnerabilities by Severity (continued)

- The total number of vulnerabilities with a critical ranking (CVSS score = 10.0) increased from 291 in 2016 to 396 in 2017. This increase is likely attributable to the higher number of vulnerabilities reported in 2017 compared to 2016.
- Trend Micro ZDI far outpaced Google Project Zero as the leading disclosing institution in reporting critical severity in 2016 with 323.
- Combining Critical and High (CVSS = 9.9 to 7.0) severity rankings, the number of vulnerabilities was 929 in 2017, an increase compared to the 693 reported in 2016. This represents 68% of the market.
- Trend Micro ZDI was the leading disclosing institution for Critical and High severity vulnerabilities with 630 in 2017, a sharp increase compared to the 378 reported in 2016.
- Google Project Zero was second in reporting Critical and High severity vulnerabilities with 178 in 2017. This represents a decline compared to the 159 reported in 2016. Google's market share dropped, with only 19% of the market, compared to 23% reported in 2016.

Source: Frost & Sullivan analysis.

Analysis of Vulnerabilities by Severity (continued)

Public Vulnerability Research Market: Reported Vulnerabilities by Severity, Global, 2016 and 2017



N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

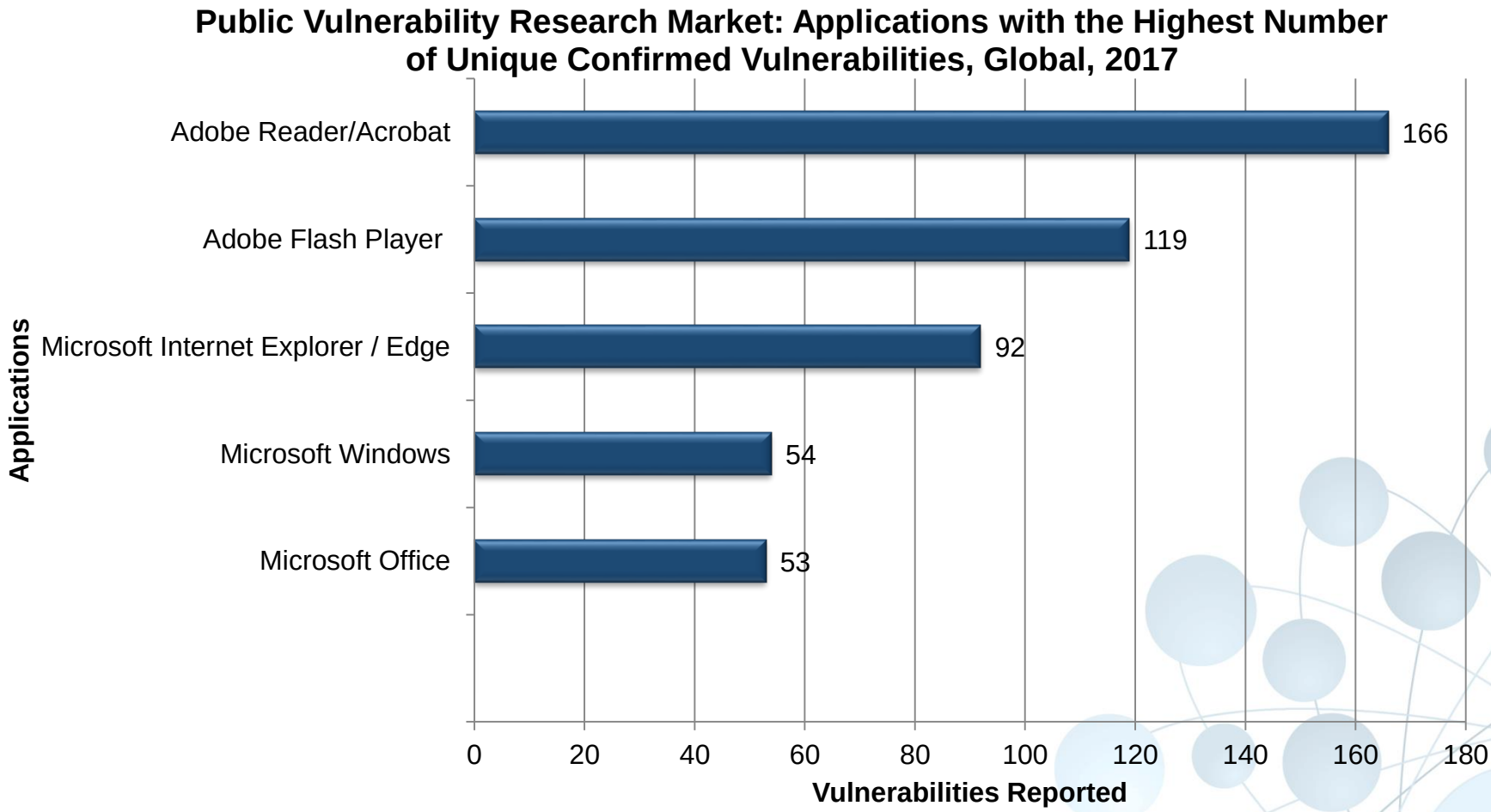
Analysis of Vulnerabilities by Severity (continued)

- Based on the total 1,522 vulnerabilities in 2017 that Frost & Sullivan included in this report:
  - Critical vulnerabilities were 396, a year-over-year increase over 2016.
  - High severity vulnerabilities were 533, a substantial increase compared to 2016.
  - Medium severity vulnerabilities increased to 259, compared to 205 in 2016.
  - Low severity vulnerabilities decreased to only 15 in 2017.
  - Vulnerabilities that were not ranked remained relatively stable at 319, down from 338 in 2016.

Source: Frost & Sullivan analysis.

Comparison of Targeted Applications

Targeted Applications



N=1,522 vulnerabilities

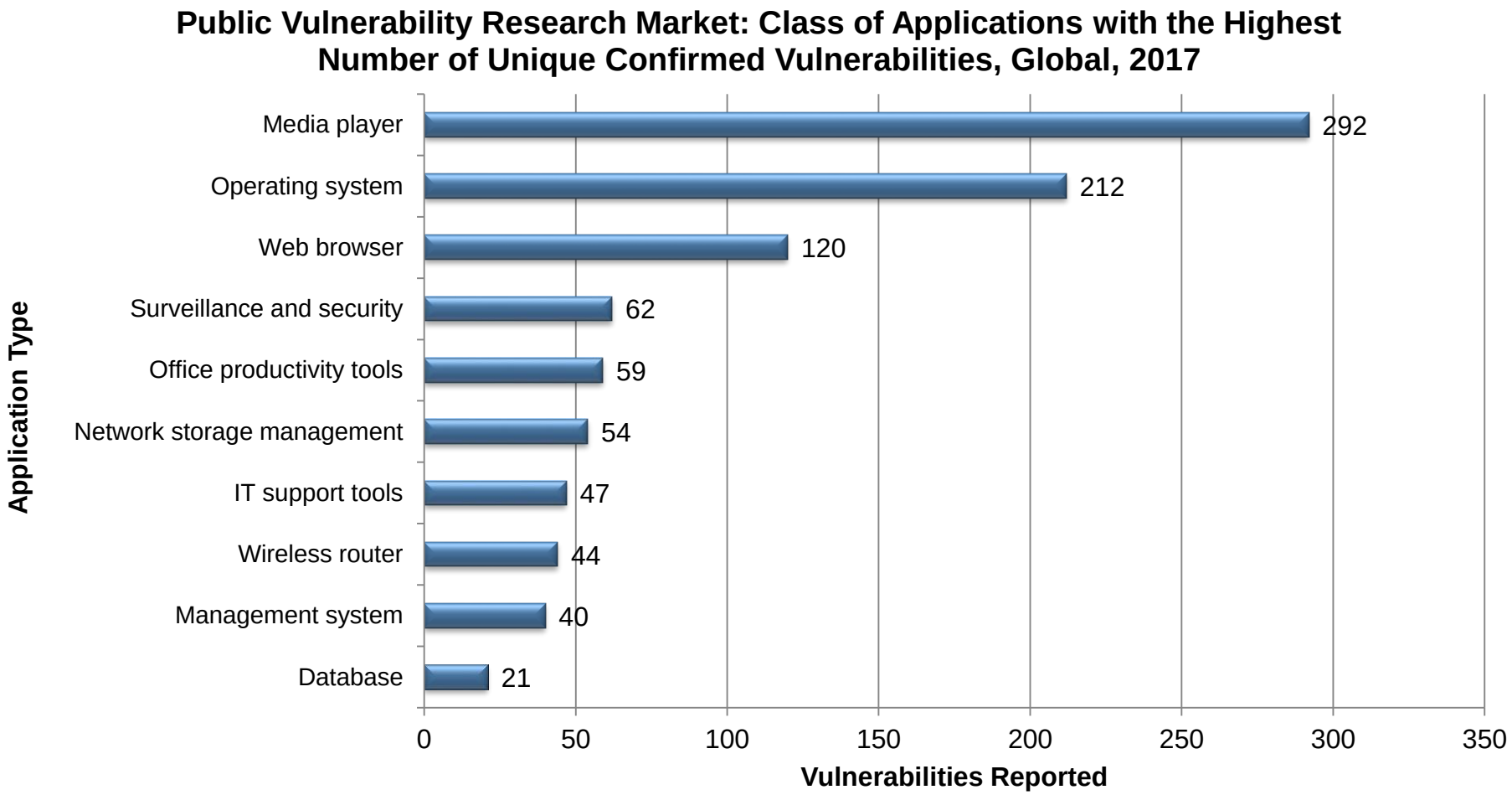
Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Analysis of Targeted Applications

- In 2017, the top five applications with the most vulnerabilities were: Adobe Acrobat Reader, Adobe Flash Player, Microsoft Internet Explorer / Edge, Microsoft Windows, and Microsoft Office.
- Overall, all reported vulnerabilities are up compared to 2016. Specifically:
  - Adobe Acrobat Reader had 166 vulnerabilities, an increase compared to 116 in 2016;
  - Adobe Flash Player had 119 vulnerabilities, compared to 101 in 2016;
  - Internet Explorer / Edge had 92 vulnerabilities, compared to 67 in 2016;
  - Windows had 54 vulnerabilities, compared to 58 in 2016;
  - Microsoft Office had 53 vulnerabilities, compared to 51 in 2016.
- Adobe's products combined accounted for 19% of the vulnerabilities in 2017.
- Client-side applications, particularly Web browsers, contained a large portion of reported vulnerabilities.

Source: Frost & Sullivan analysis.

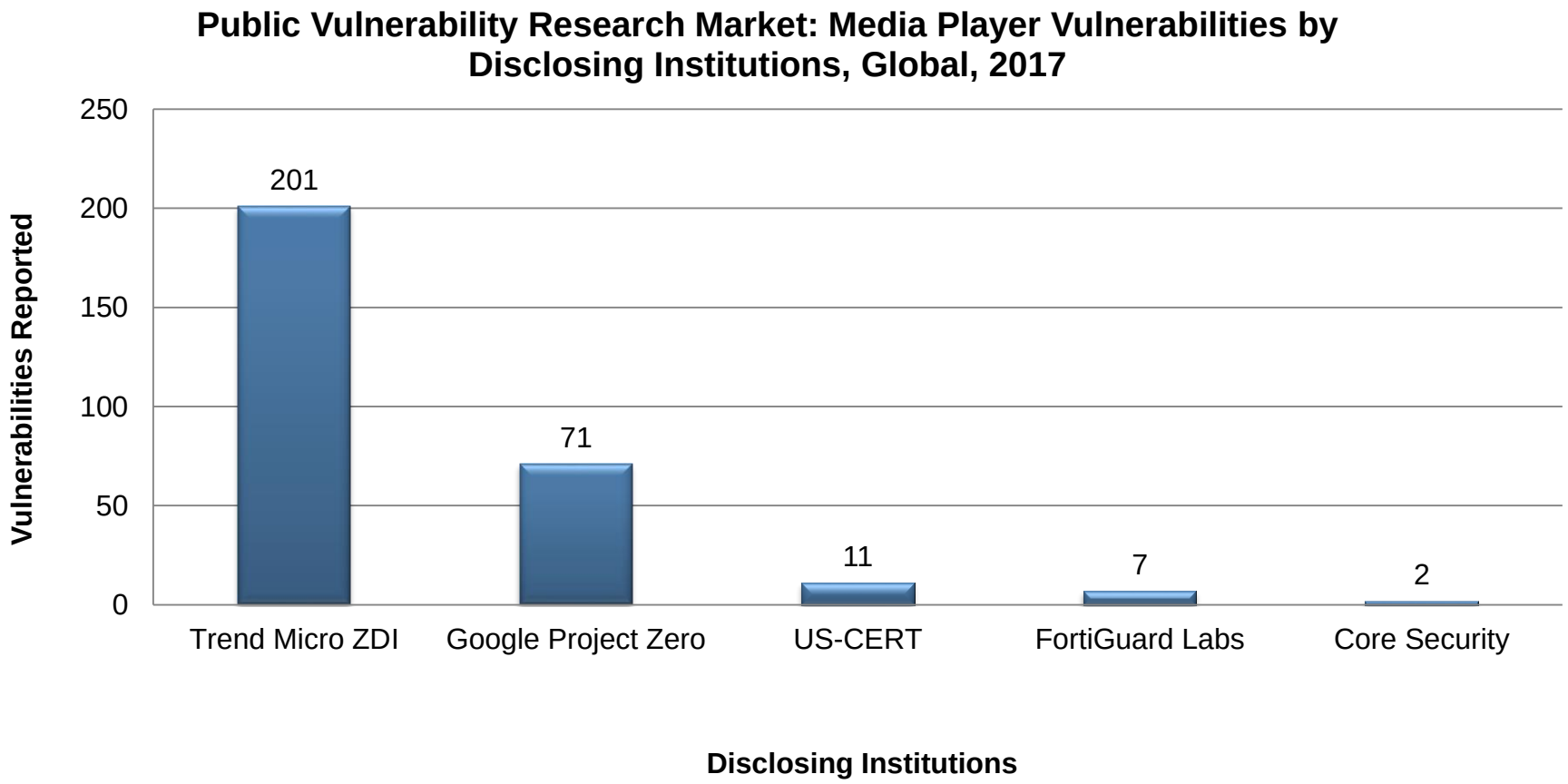
Top Targeted Class of Applications



N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

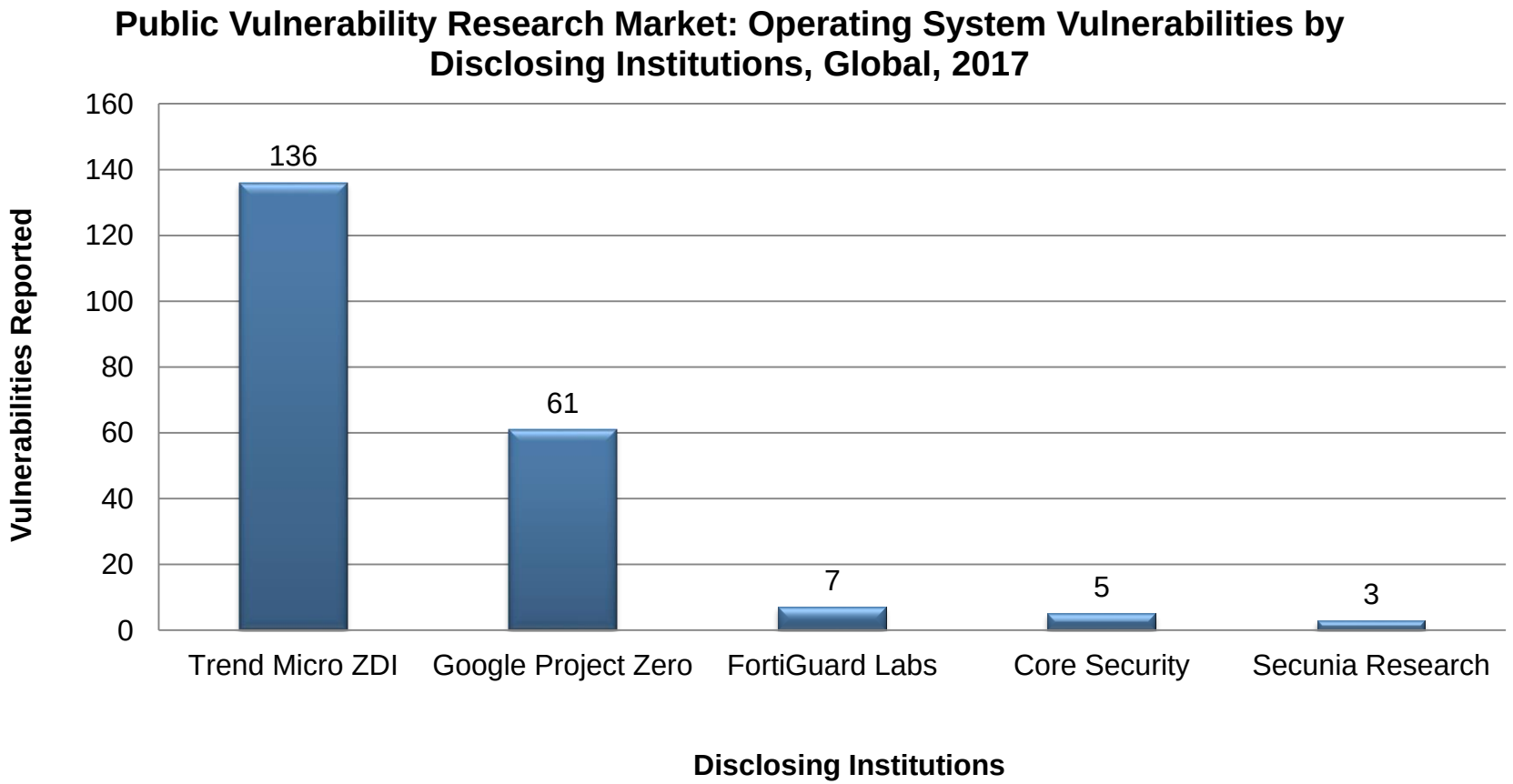
Disclosing Institutions: Media Player Vulnerabilities



N=292 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

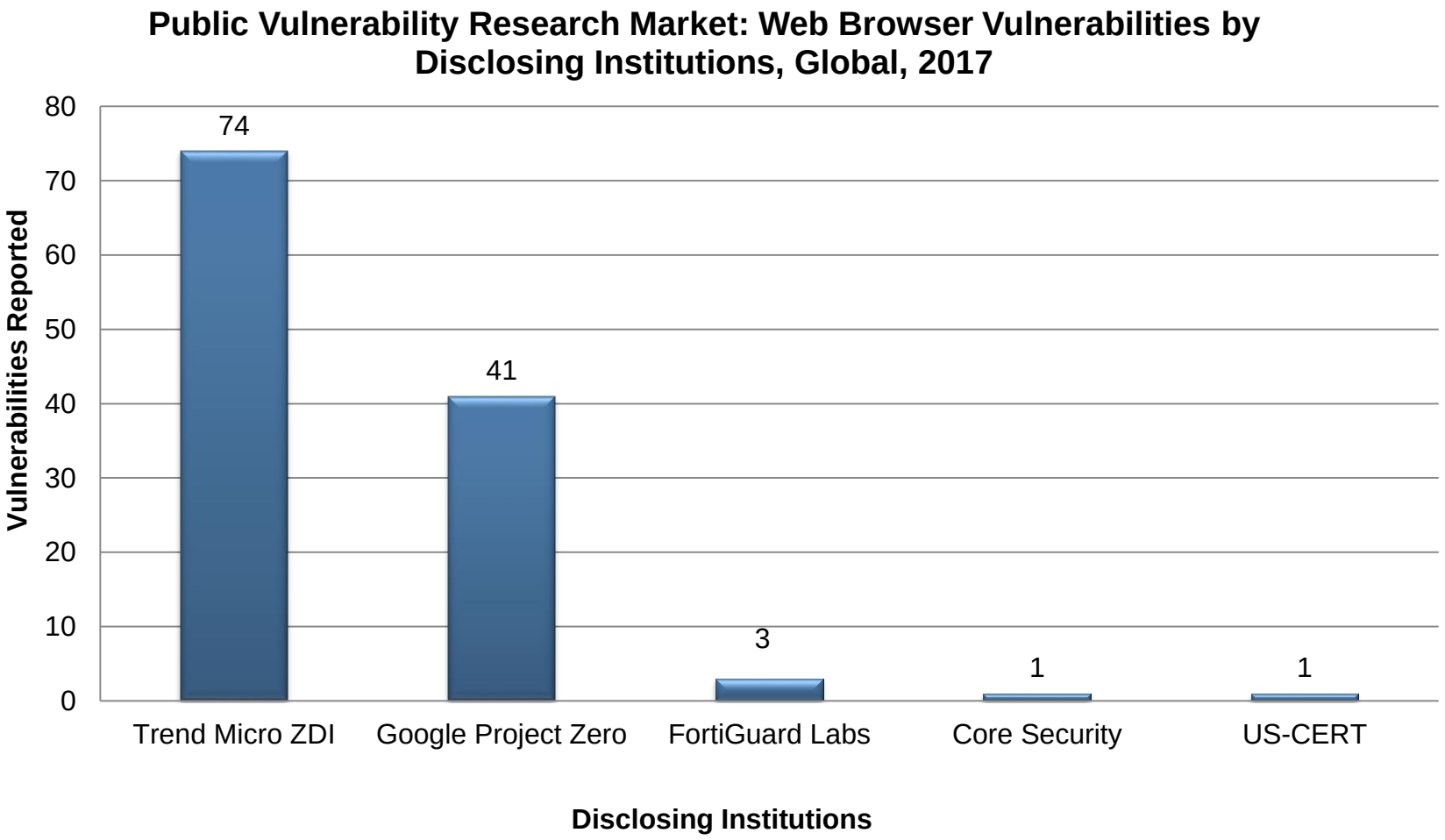
Disclosing Institutions: Operating System Vulnerabilities



N=212 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Disclosing Institutions: Web Browser Vulnerabilities



N=120 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

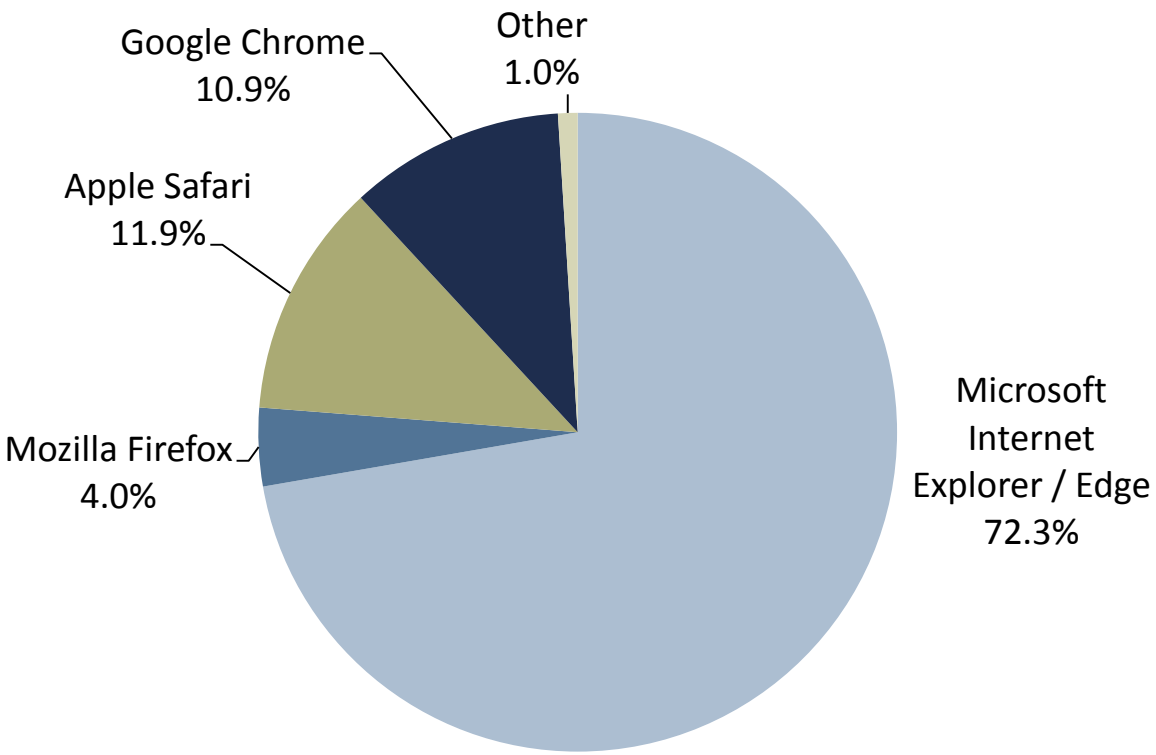
Analysis of Targeted Applications by Class

- Media players had 292 vulnerabilities in 2017, with Adobe Flash accounting for the bulk of these.
- Trend Micro ZDI was the leading disclosing institution for media players, with Google Project Zero second.
- Operating systems were the second highest with 212 vulnerabilities, up considerably since 2016, where only 177 were reported. These are predominantly various versions of Microsoft Windows. Researchers continue to focus attention in this area.
- Trend Micro ZDI were the dominant disclosing institutions for operating systems.
- The Web browser was the most targeted application within Web applications with 120 discovered vulnerabilities.
- Trend Micro ZDI was the dominant disclosing institution for Web browser vulnerabilities.

Source: Frost & Sullivan analysis.

Targeted Web Browser Type

Public Vulnerability Research Market: Percent of Reported Vulnerabilities by Web Browser Type, Global, 2017



N=120 vulnerabilities

Note: All figures are rounded. The base year is 2017. 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 2017 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.

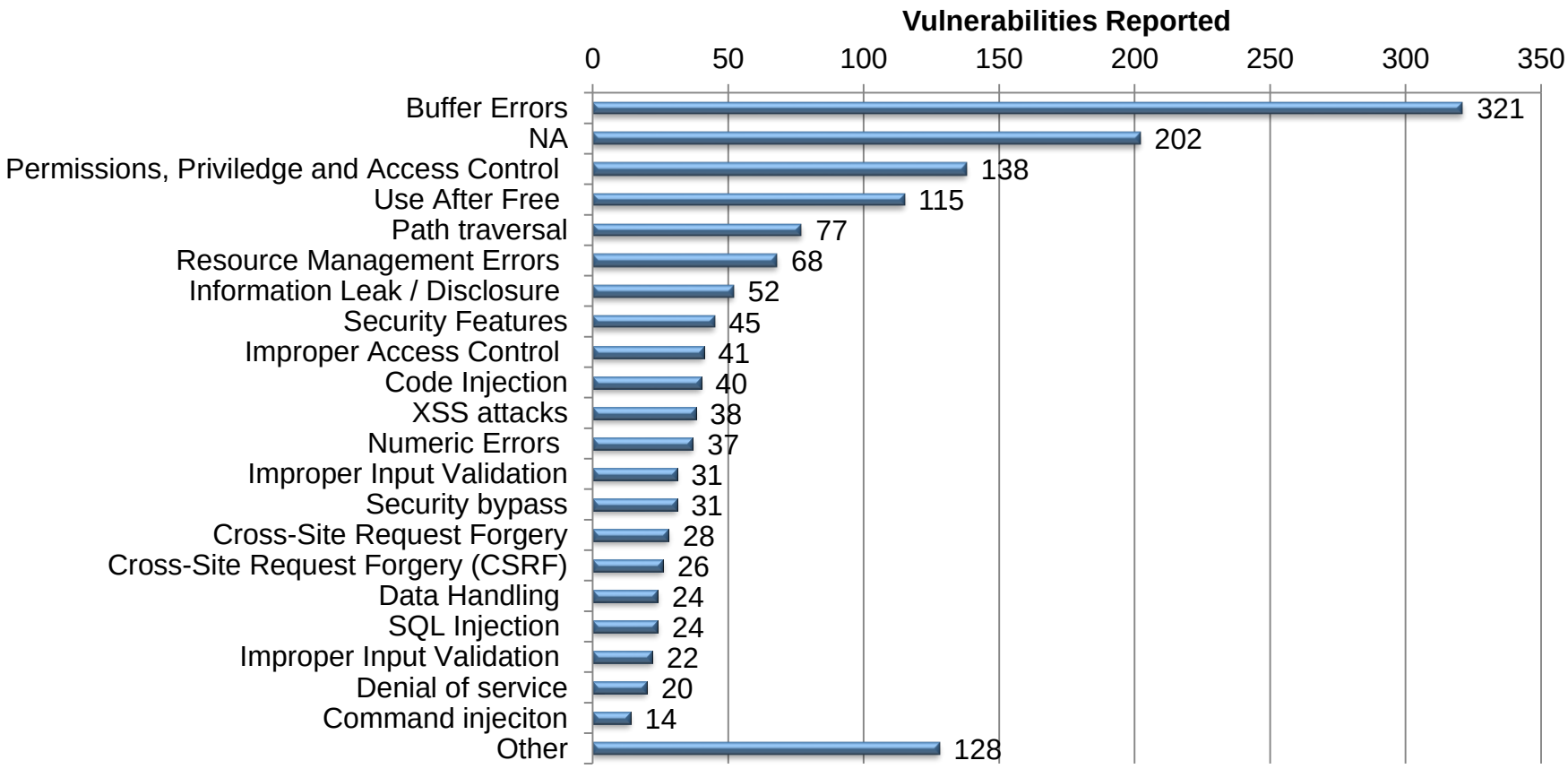
Vulnerability Definitions (continued)

- **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 (2017)

Public Vulnerability Research Market: Reported Vulnerabilities by Top Flaw Type, Global, 2017

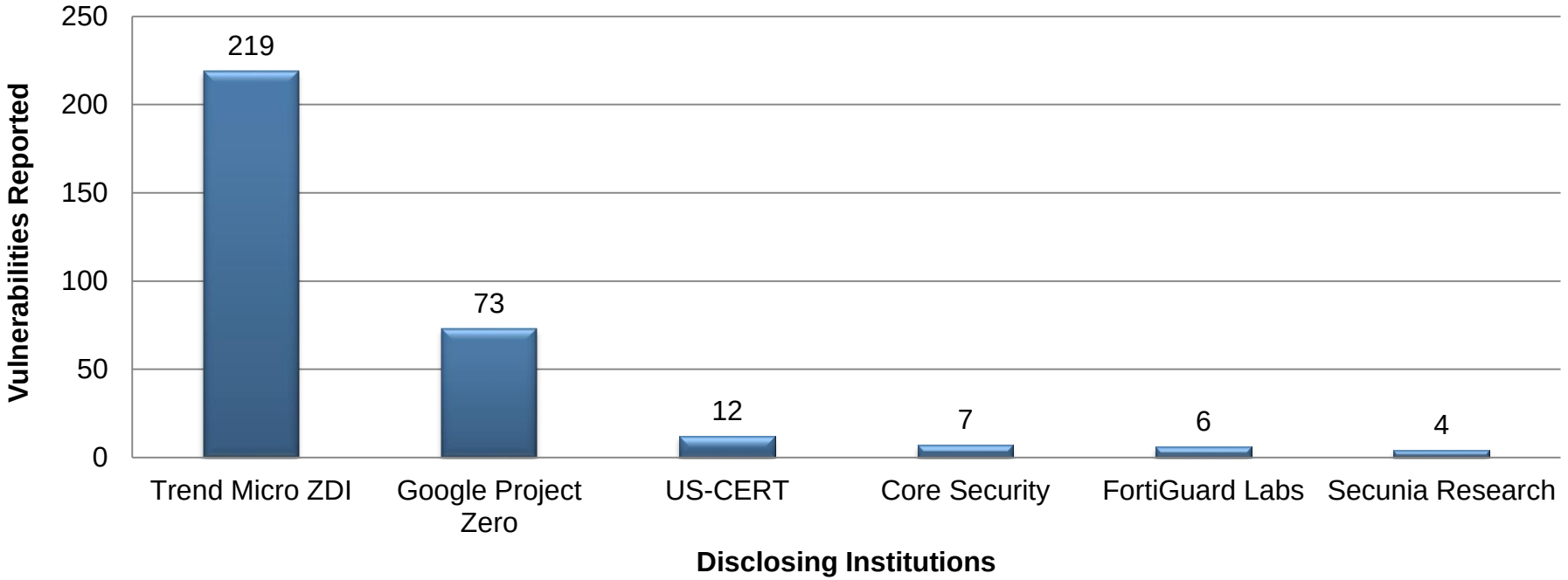


N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Disclosing Institutions: Buffer Errors

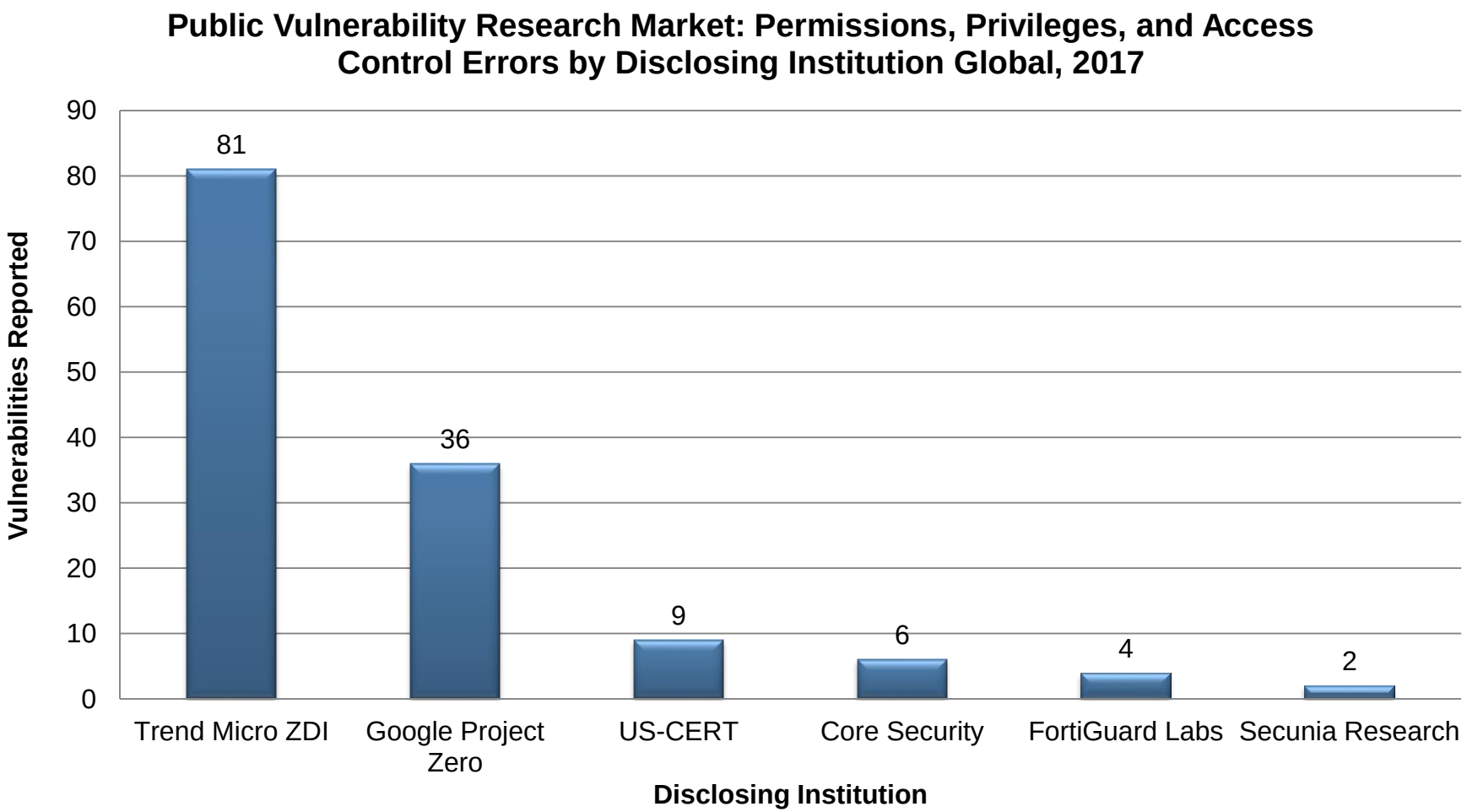
Public Vulnerability Research Market: Reported Buffer Errors by Disclosing Institutions Global, 2017



N=321 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

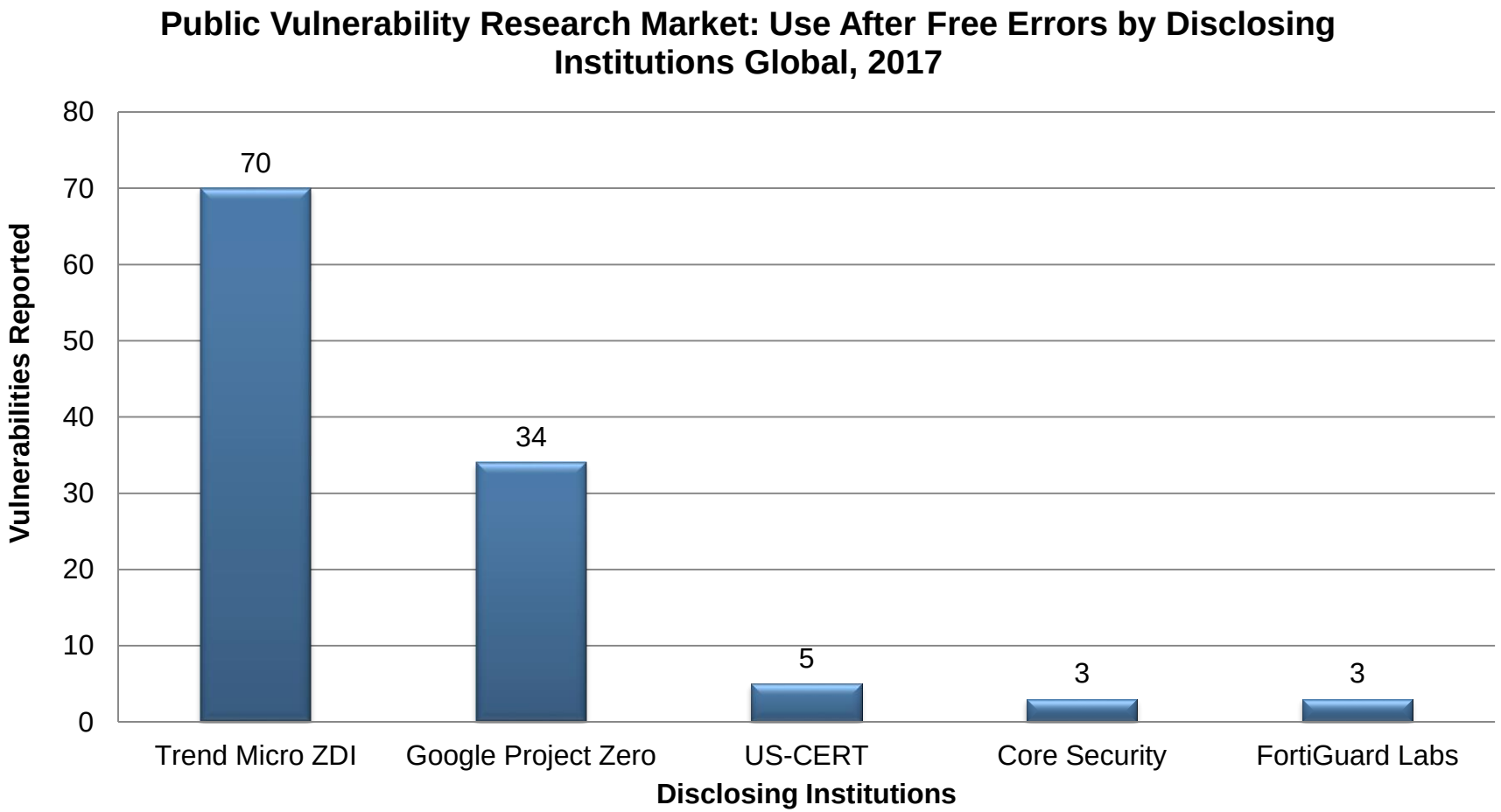
Disclosing Institutions: Permissions, Privileges, and Access Control Errors



N=138 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Disclosing Institutions: Use After Free Errors

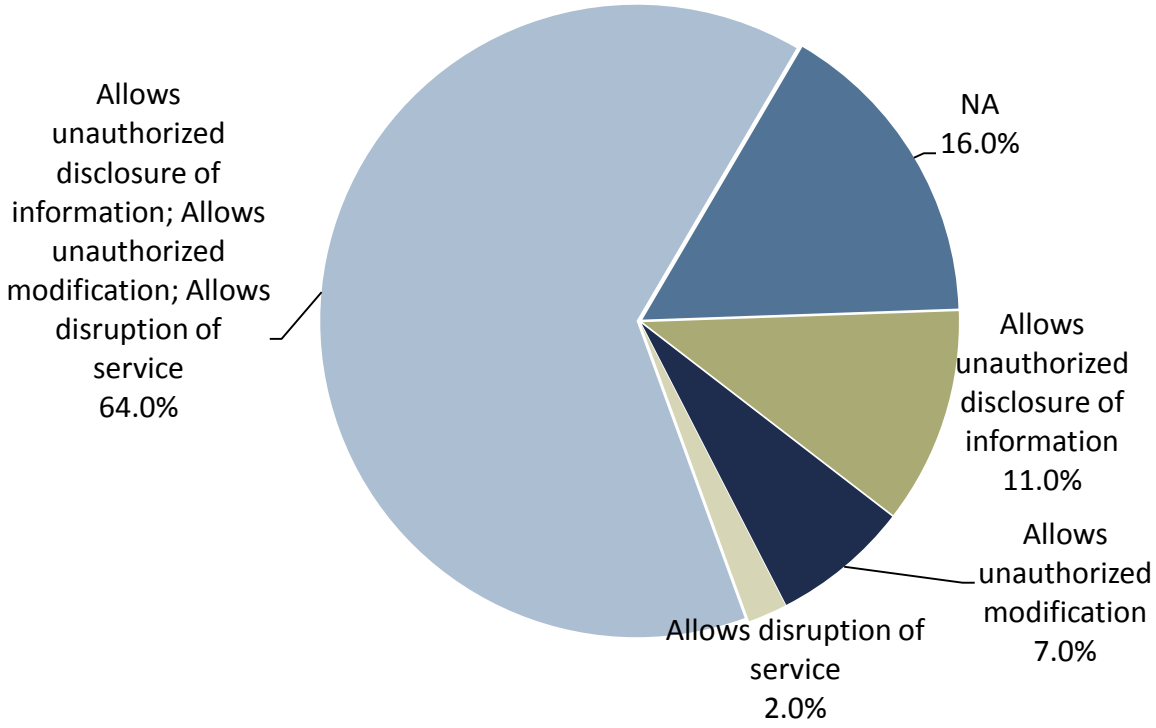


N=115 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Top Impact Type

Public Vulnerability Research Market: Percentage of Vulnerability Reports by Associated Impacts, Global, 2017



N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

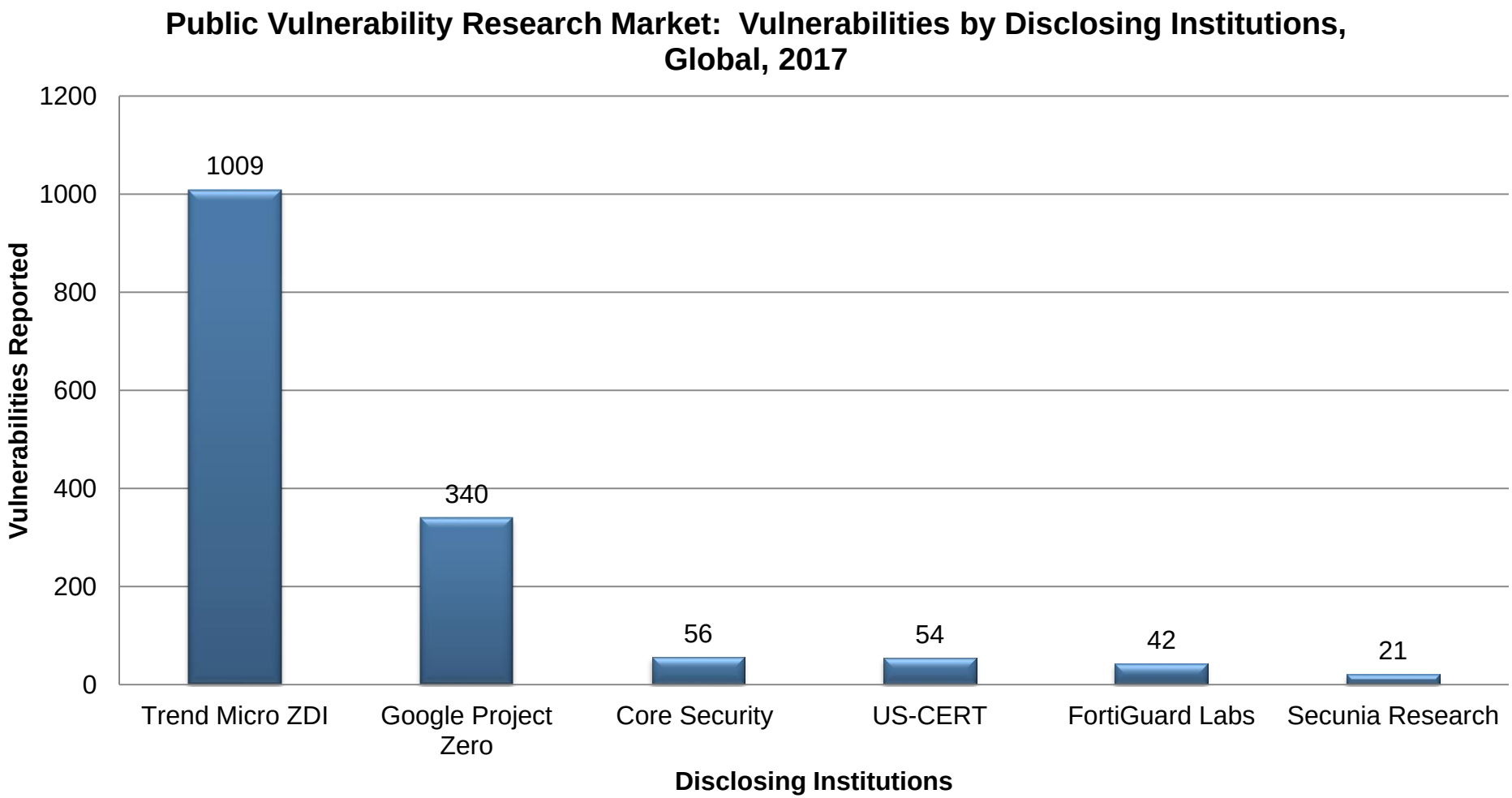
Analysis of Impact Types

- The NVD was the final authority used to report the impacts in the tables.
- Buffer overflow errors were the most common vulnerability flaw in 2016 and remained so in 2017. Trend Micro ZDI found 219 incidents of buffering errors in 2016, followed by Google Project Zero which found 73 vulnerabilities related to buffering errors.
- If a vulnerability was found, 64% of the time the impact was likely to be exploited to deny service, modify files and allow unauthorized access. This could be classified as a jailbreak vulnerability.

Source: Frost & Sullivan analysis.

Competitive Analysis

Competitive Analysis Vulnerabilities

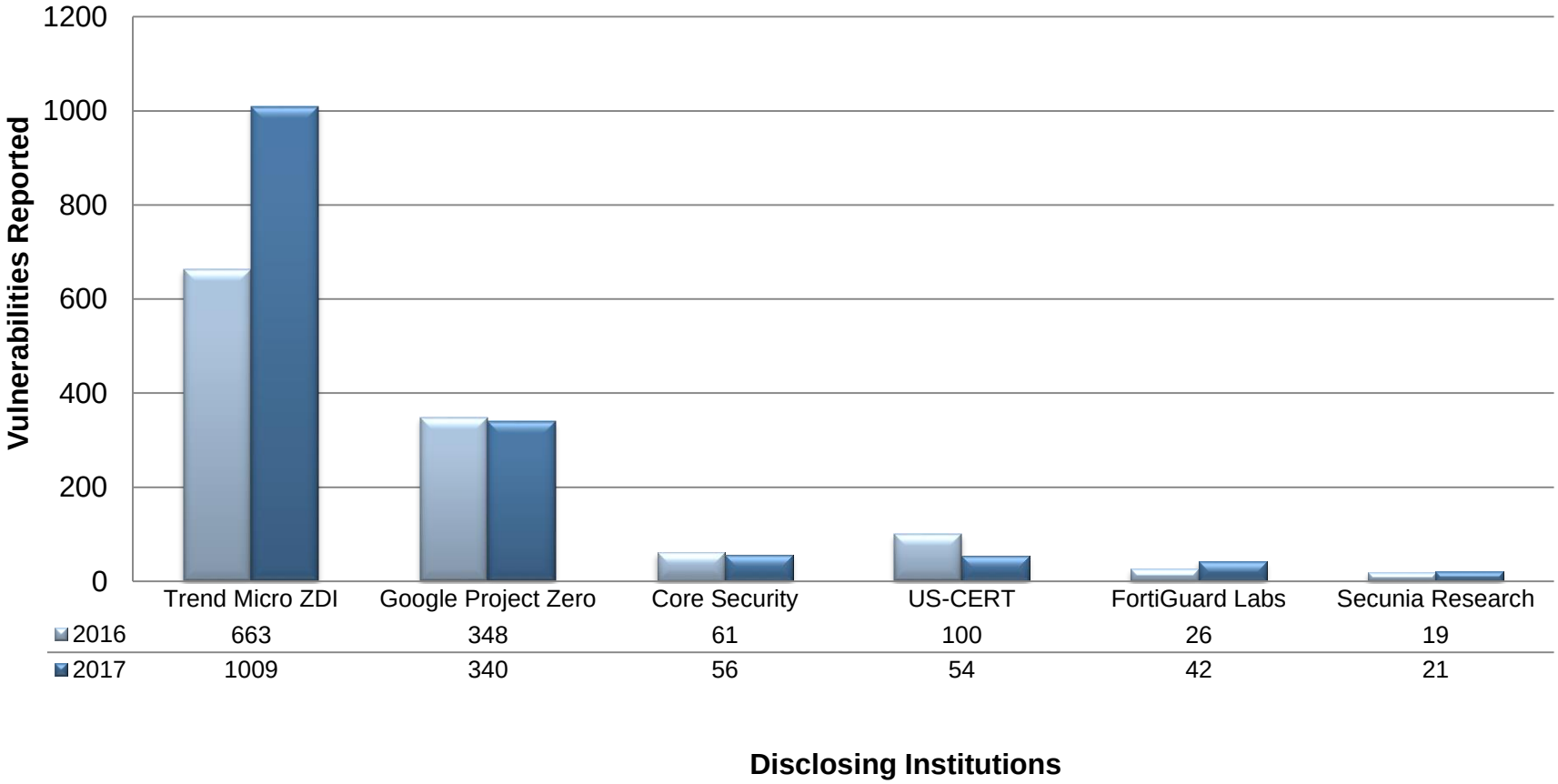


N=1,522 vulnerabilities

Note: All figures are rounded. The base year is 2017. Source: Frost & Sullivan analysis.

Competitive Analysis Vulnerabilities (continued)

Public Vulnerability Research Market: Total Vulnerabilities by Disclosing Institutions, Global, 2016 and 2017



Note: All figures are rounded. The base year is 2017. 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 2017, Trend Micro ZDI reported the most verified vulnerabilities with 1009. Trend Micro ZDI reported 66.3% of total vulnerabilities.
- Google Project Zero follows with 340 vulnerabilities in 2017, accounting for 22.3% of total vulnerabilities reported.

Source: Frost & Sullivan analysis.

Profiles of Security Platform Providers Offering Public Vulnerability Disclosure

Core Security

- Core Security, the result of Courion's December 2016 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.
- 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, 2016, 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 2016, 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)

- 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.

Secunia Research (Flexera)

- In September 2016, Flexera announced plans to acquire Secunia, and ultimately the deal was completed in December 2016.
- 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 2016, 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.

Trend Micro Zero Day Initiative

- In March 2016, Trend Micro acquired TippingPoint, one of the original pioneers of the IPS market. The acquisition included the Zero Day Initiative as well as the TippingPoint DVLabs team.
- 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.
- The Zero Day Initiative 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.”
- While the Zero Day Initiative is working with vendors, Trend Micro customers are protected ahead of the vendor patch or workaround.
- Trend Micro 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 Trend Micro.
- Additionally, Trend Micro ZDI 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.

Source: Frost & Sullivan analysis.

Trend Micro 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 today as they were at the inception of the program (from the Zero Day Initiative Website):
  - Extend the 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 Trend Micro 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 the Zero Day Initiative and from the fully vetted vulnerabilities reported by individual contributors are used in TippingPoint's Digital Vaccine service and have been 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.

Appendix

Vulnerability Database Sources (for 2017)

- Current Network Security Advisories | Core Security
- FortiGuard Security Advisories | FortiGuard.com
- Google Project Zero - Monorail
- Computer Security Research - Secunia
- Trend Micro Zero Day Initiative
- US CERT Vulnerability Notes

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