Quantifying the Public Vulnerability Market

Vulnerability Disclosures, Impact Severity, and Product Analysis

July, 2020

Information Classification: General

Research from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD)

Overview

Omdia conducted comprehensive comparative research and analysis surrounding 11 organizations that disclose information security vulnerabilities. As a component of this research, Omdia cross-referenced the data from these vendors against the information organized and published by various government agencies, including:

- The MITRE Corporation
- The National Institute of Standards and Technology (NIST)
- The United States Computer Emergency Response Team Coordination Center (US CERT/CC)
  - While listed with other reporting organizations, the US CERT/CC is a U.S. government agency, not a security vendor of any kind

Research Scope

The scope of Omdia's analysis used the following constraints:

- Vulnerabilities will only be credited to a vendor if they are ultimately responsible for managing the disclosure of the vulnerability
- All vulnerabilities must have been disclosed within the 2019 calendar year
- All vulnerabilities must have been assigned a Common Vulnerability and Exposure (CVE) number.
- Disclosed vulnerabilities with associated CVEs that were not credited to the organizations within our scope were not incorporated or discussed as part of our overall analysis.
- In the instances where credit for a vulnerability was claimed by two or more vendors, we granted credit to each vendor making the claim, as there was no way to independently validate credit.
  - **1,067** vulnerabilities were claimed once, and **14** vulnerabilities claimed twice.
  - This resulted in a total of **1,081** unique and verified vulnerabilities.
- As we attributed credit for each vulnerability to all vendors who claimed it, the resulting total number of all verified vulnerabilities claimed by the 11 research organizations for 2019 is ***1,095.***

Analysis Methodology

The data collected for this report stems from multiple sources, including:

- Primary Internal Research
- Individual Vendor Interviews
- Open Source Publications
- Publicly Disclosed Reports

Omdia collected all publicly available vulnerability data from each of the organizations listed in the executive summary and assigned credit for each vulnerability. However, in order to be attributed credit for a listed vulnerability an organization had to be responsible for effectively managing its disclosure, meaning that the organization directly oversaw the release of the vulnerability.

- Credit for managing a vulnerability ***was not assigned*** to a vendor simply because it was listed on their publicly facing advisory website.

Omdia then collected data on all verified vulnerabilities during 2019 using the NIST NVD data feeds, and used this data as the baseline for vendor comparison.

- To be considered verified, all vulnerabilities in our analysis had to have an associated CVE number in order to prevent rejected or duplicated entries from being introduced into the analysis, as well as have a CVSS value assigned by the NVD.
- Vulnerabilities without a CVE, while credited to the vendor listing them, could not be used in our analysis.

The CVSS and CWE metrics assigned by the NVD allowed Omdia to conduct a comparative analysis of the performance of all vendors, the severity of the vulnerabilities they disclosed, and the attack methodology of the vulnerabilities each vendor was credited with.

Vulnerability Market Analysis

A vulnerability is a weaknesses, error, defect, flaw, or bug that poses a threat to the confidentiality, integrity, and availability of data within an information system. Adversaries seek to take advantage of any vulnerabilities present in hardware, software, and firmware, as they can be exploited in ways that compromise the systems on which they reside. The greater the window of time between the discovery of a vulnerability, its disclosure, and ultimate remediation, the more time a potential hacker has to exploit the vulnerability.

Vulnerabilities that exist, but are unknown to the affected vendor, are commonly referred to as zero-day vulnerabilities. Zero-day vulnerabilities simultaneously pose the greatest threats to information security, and are viewed as the greatest prize for cyber criminals to attain and share. As vulnerabilities can only be addressed once they are discovered and shared with the affected vendor, there is an incentive to report a vulnerability as quickly as possible. Even if a vulnerability is mitigated through a security patch, the threat remains for every system that hasn't been updated.

As more product vendors, security organizations, and individual researchers contribute to the process, the associated threats introduced by vulnerabilities can be mitigated with greater efficacy. The potential impact of these vulnerabilities can vary greatly, as some security flaws may merely be annoying, others are critical enough to have potentially catastrophic consequences for the vulnerable systems and its users.

To conduct comprehensive analysis on any vulnerability, there are several characteristics and values that need to be identified first in order to cross reference them across reporting organizations:

- Common Vulnerability and Exposure (CVE) values
  - Unique identifier given to each vulnerability by a CVE Numbering Authority (CNA)
- Common Weakness Enumeration (CWE) values
  - Preliminary identifier used to categorize and define common software weaknesses
- Common Vulnerability Scoring System (CVSS) values
  - Numerical score reflecting the severity of the vulnerability

Results

The associated CVSS score attached to each vulnerability by the NVD provides organizations with a visible metric by which to gage the severity associated to any vulnerability, and help prioritize any threat remediation strategies.

Critical threats are those that can have potentially catastrophic impacts on an organization's information security. These threats typically surround unauthorized root-level access, and can result in the unauthorized modification/disclosure of data, or denial of service (DoS). Threats are often elevated to this level if an attacker can gain access without any special conditions or knowledge.

- Critical scoring vulnerabilities accounted for roughly 14.2% of all disclosed threats.

High scored threats can also have substantially damaging effects to the information security of an organization. However, these vulnerabilities are traditionally more challenging to exploit, as they require certain conditions be met first. Although, any exploitation can still result in privilege escalation of loss of access to data.

- High scoring vulnerabilities accounted for the majority of those disclosed, comprising 59.2% of all vulnerabilities.

Medium vulnerabilities can have negative impacts on an organization's data security, but often more challenging to exploit, as specific requirements must be met in order to effectively exploit the vulnerability.

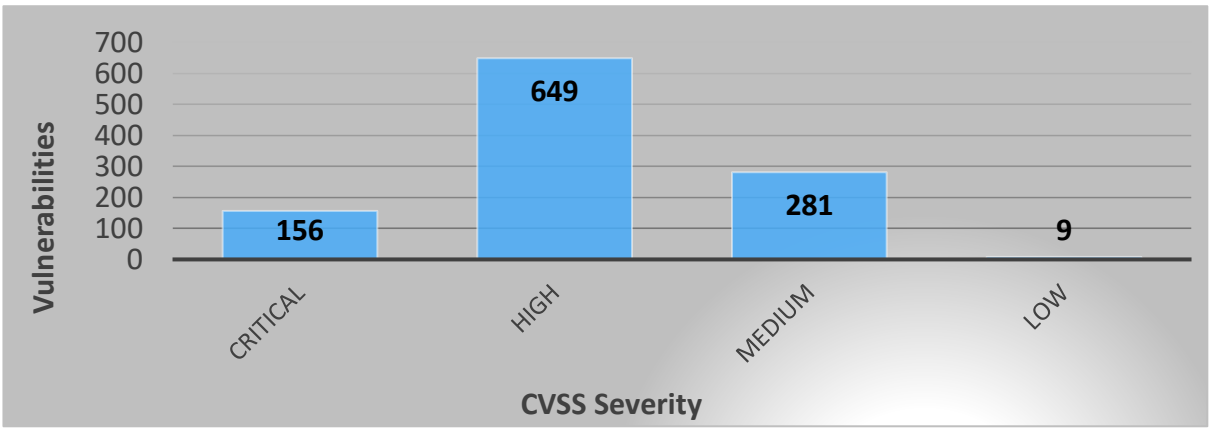
- Medium scoring vulnerabilities were ranked second, comprising 25.6%

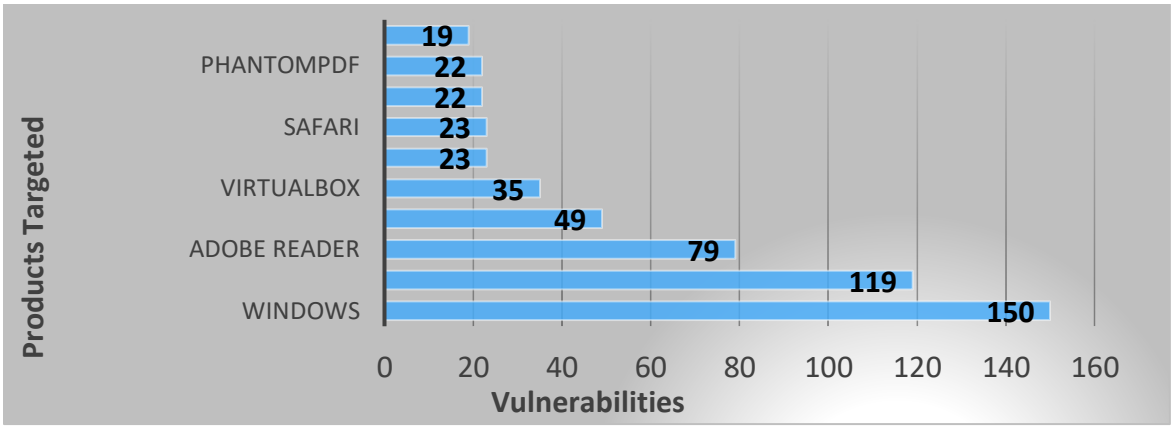
Low-N/A scored vulnerabilities have little to no impact on the data security for an organization, and pose more of an annoyance than a legitimate threat.

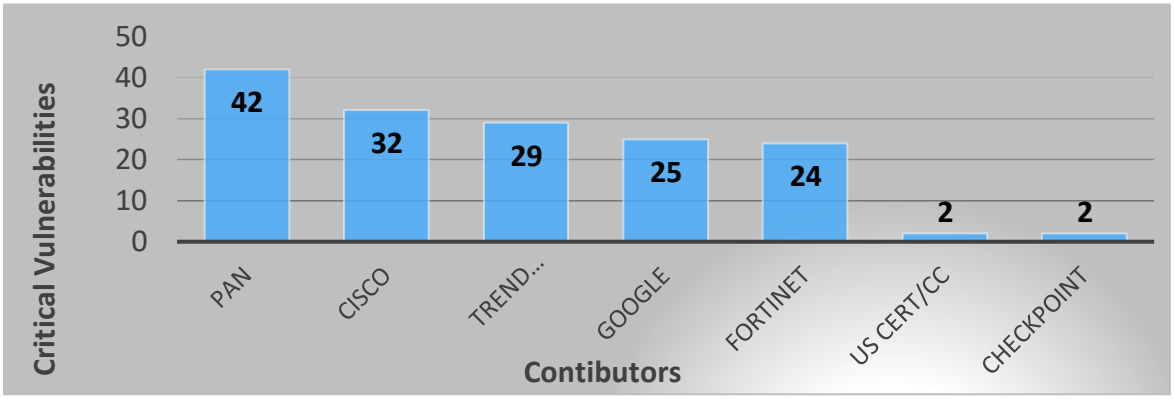
- These low-grade threats accounted for less than 1% of all disclosed vulnerabilities.

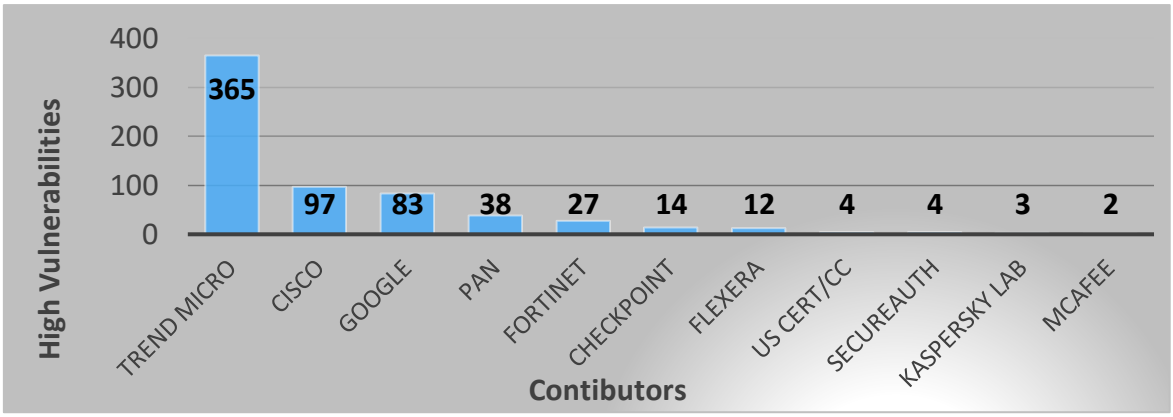
Conclusion

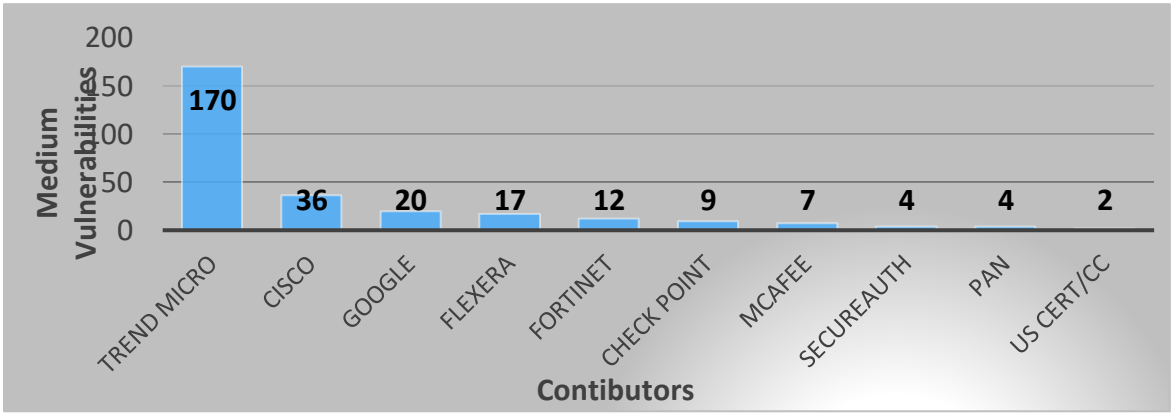
Each of the organizations analyzed in this research is contributing towards the efforts of discovering and disclosing information security vulnerabilities. It is through the diligence of vendors such as these that the security of data can become more robust, as flaws can only begin to be addressed once they are acknowledged. As technology continues to evolve, it is imperative that this work continue if comprehensive security is to be achieved through the responsible management of vulnerabilities.

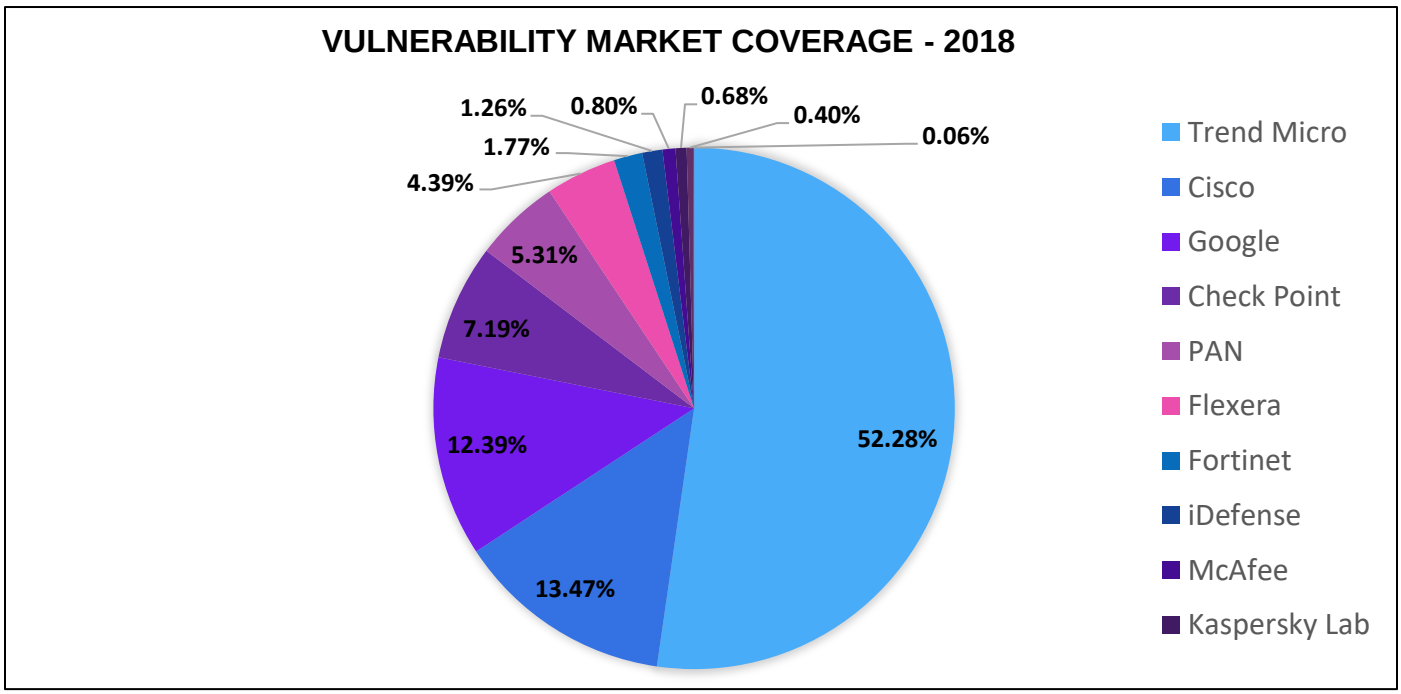



Products Targeted
PHANTOMPDF
SAFARI
VIRTUALBOX
ADOBE READER
WINDOWS
19
22
22
23
23
35
49
79
119
150
0
20
40
60
80
100
120
140
160
Vulnerabilities

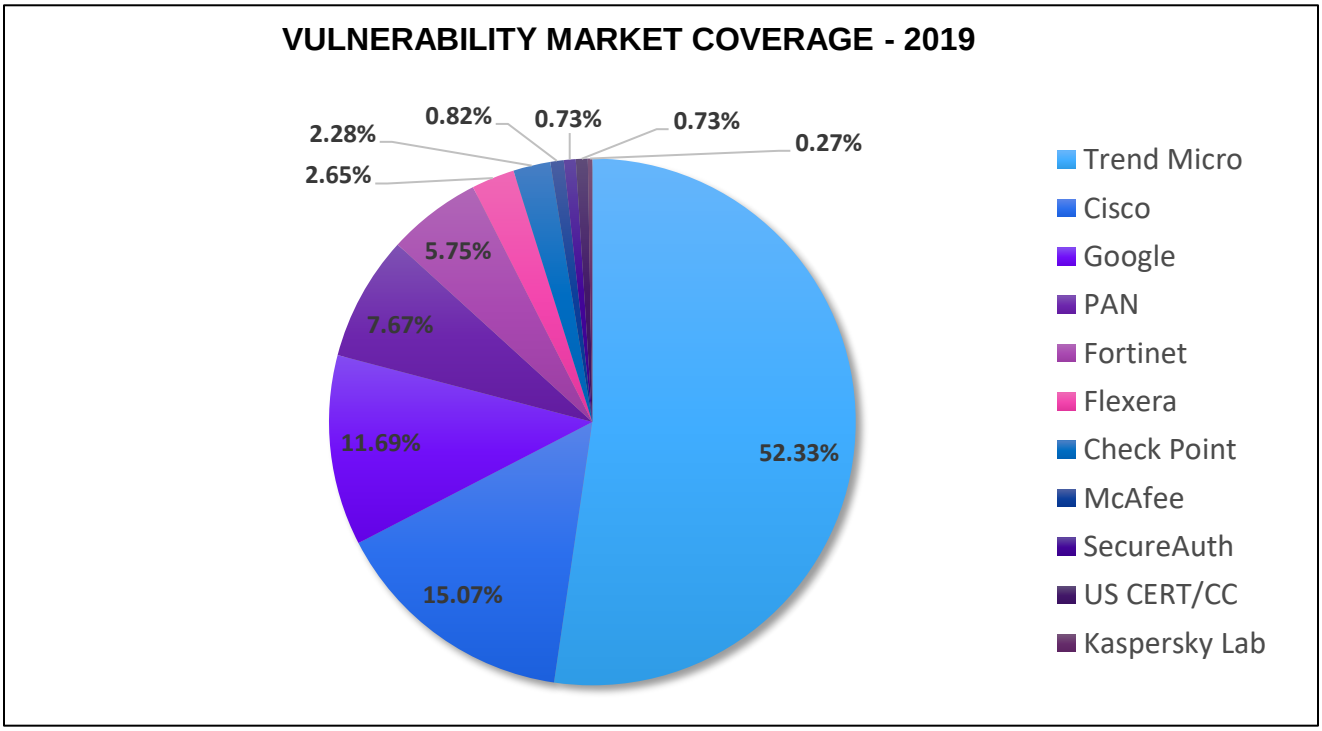

Critical Vulnerabilities
50
40
30
20
10
0
42
32
29
25
24
2
2
PAN
CISCO
TREND...
GOOGLE
FORTINET
US CERT/CC
CHECKPOINT
Contibutors


High Vulnerabilities
400
300
200
100
0
365
97
83
38
27
14
12
4
4
3
2
TREND MICRO
CISCO
GOOGLE
PAN
FORTINET
CHECKPOINT
FLEXERA
US CERT/CC
SECUREAUTH
KASPERSKY LAB
MCAFEE
Contibutors


Medium Vulnerabilities
200
150
100
50
0
170
36
20
17
12
9
7
4
4
2
TREND MICRO
CISCO
GOOGLE
FLEXERA
FORTINET
CHECK POINT
MCAFEE
SECUREAUTH
PAN
US CERT/CC
Contibutors



IHS Markit Research - 2018	Vulnerabilities Managed	Average of Base Score	Average of Exploitability Score	Average of Impact Score
Trend Micro	916	7.64	2.49	5.04
Cisco	236	7.83	2.34	5.33
Google	217	6.31	1.79	4.43
Check Point	126	7.45	2.61	4.79
PAN	93	7.22	2.48	4.66
Flexera	77	7.10	2.70	4.31
Fortinet	31	7.81	2.19	5.50
iDefense	22	7.70	2.61	5.01
McAfee	14	7.49	2.06	5.26
Kaspersky Lab	12	8.04	2.46	5.52
CERT/CC	7	8.53	3.74	4.76
SecureAuth	1	7.80	1.80	5.90
Total	1752	7.45	2.40	4.95



Omdia Research - 2019	Vulnerabilities Managed	Average of Base Score	Average of Exploitability Score	Average of Impact Score
Trend Micro	573	7.57	2.41	5.04
Cisco	165	7.90	2.91	4.91
Google	128	8.18	2.67	5.39
PAN	84	8.58	3.69	4.86
Fortinet	63	8.24	2.82	5.33
Flexera	29	6.51	3.54	2.92
Check Point	25	7.58	2.82	4.68
McAfee	9	6.09	1.19	4.81
SecureAuth	8	6.85	2.60	4.14
US CERT/CC	8	7.73	2.33	5.33
Kaspersky Lab	3	7.80	1.80	5.90
Grand Total	**1095**	**7.76**	**2.66**	**4.99**

Omdia provided access to both studies in order to provide a comparative annual analysis.

Author

Tanner Johnson, Senior Analyst, Cybersecurity

tanner.johnson@omdia.com

Copyright notice and disclaimer

CONTACT US

omdia.com

askananalyst@omdia.com