Vulnerability QuickView
2016 Year End

Risk Based Security, Inc.

January 2017

Vulnerability Statistics - Better Data Matters

Gathering and reporting vulnerability intelligence is not an exact science. Discovering the new and ever-growing number of sources is a daily challenge and can be even more difficult to interpret correctly. Incomplete information, constant updates and revisions, mis-interpretation, and errors in reporting, can all contribute to a level of confusion regarding the impact, severity and risk a vulnerability represents.

It is important that vulnerability statistics be presented in a clear, responsible and standardized manner with the appropriate definitions, disclaimers, and notes. With full disclosure in mind, VulnDB counts only distinct vulnerabilities. Meaning, if a product includes vulnerable code from third-party dependencies it is not treated as a new vulnerability unlike the reporting of some vulnerability intelligence sources.

Further, the CVE/NVD numbers reflected in this report are the total number of unique vulnerabilities published in each year that have an associated CVE ID. This number is lower than the total number of assigned CVE identifiers, which includes many RESERVED IDs that are not associated with any published vulnerabilities.

Also note that of all the published vulnerabilities in 2016 with CVE IDs, 1,945 are still marked as RESERVED in the CVE dictionary and are, therefore, currently missing from CVE/NVD.

No matter the author, no matter the source, vulnerability intelligence and the resulting statistics must be interpreted carefully. We encourage you to reach out to your vulnerability intelligence provider and/or your network scanning service and ask about their vulnerability data sources, update timeliness, and research methodology. The security of your information assets depends on it.

QuickView
VulnDB

- 2016 is the new all time high with VulnDB reaching 15,000 vulnerabilities as of January 23, 2017.
- The number of 2016 vulnerabilities reflects a 85.3% increase compared to the low (8,094) reported in 2011.
- The number of vulnerabilities published by CVE/NVD decreased by 8.2% in 2016 compared to their high-mark of 9,088 in 2014.
- VulnDB published 6,659 more vulnerabilities than CVE/NVD in 2016.
- CVSSv2 scores above 9.0 account for 21.3% of all 2016 vulnerabilities.
- Coordinated Disclosure climbs to 44.9% of the total 2016 vulnerabilities.
- Major vendors show steady increase in vulnerabilities since 2009.
- Web-related vulnerabilities accounted for 53.5% of total in 2016.
- Data Integrity impacted by 66.9% of 2016 vulnerabilities.
- 32.8% of 2016 vulnerabilities have public exploits.
- 81.3% of 2016 vulnerabilities have a documented solution.
- 48.9% of 2016 vulnerabilities can be exploited remotely
- 1.3% of 2016 vulnerabilities were coordinated through vendor bug bounty programs. 4.8% were through 3rd party bug bounty programs.
- SCADA vulnerabilities increased 84.8% over 2014.

VulnDB
EVERYTHING IS VULNERABLE

Our Challenge

Exploiting software vulnerabilities has been the number one breach type year over year since taking over the top spot from stolen laptops in 2011. [https://cyberriskanalytics.com/]

Organizations today face a heavy and constant workload to patch software vulnerabilities, but as heavy as it is, most organizations are not aware of all the vulnerabilities impacting their assets. They simply rely on incomplete data.

Vulnerability free software does not appear to be in our near-term future. At Risk Based Security we added 41 new vulnerabilities to our vulnerability database each and every day in 2016.

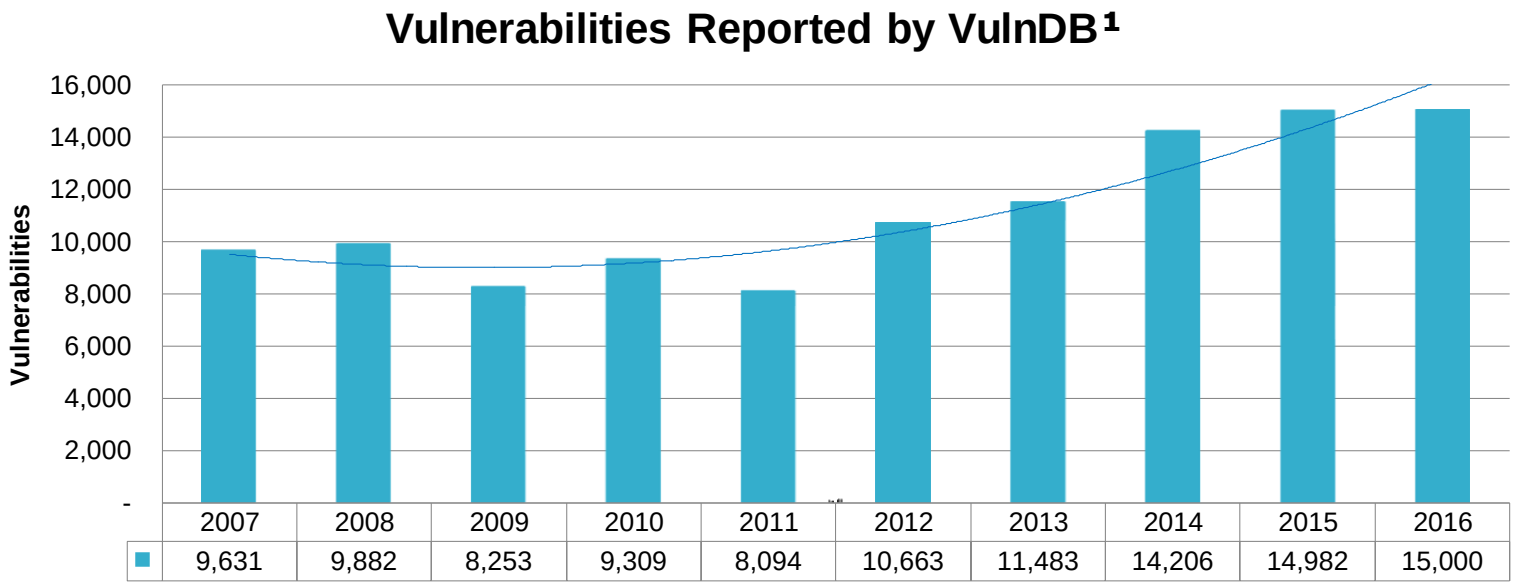
All organizations must have a proactive plan to address not only the newly released vulnerabilities, but to ensure they have addressed vulnerabilities from previous years. They also need to constantly stay updated on the release of fixes for previously unpatched vulnerabilities or changes to the risk rating for unaddressed vulnerabilities like the release of exploit code.

A simple review of the numerous data breaches reported each day sends a clear signal that many organizations are not keeping pace.

Internal teams attempting to locate, research, and verify vulnerability data is taking valuable resources from the fight to implement solutions, leaving your network at risk. Relying on a scanner to direct your vulnerability management program is a failing proposition.

The following information was derived from Risk Based Security's VulnDB Solution.

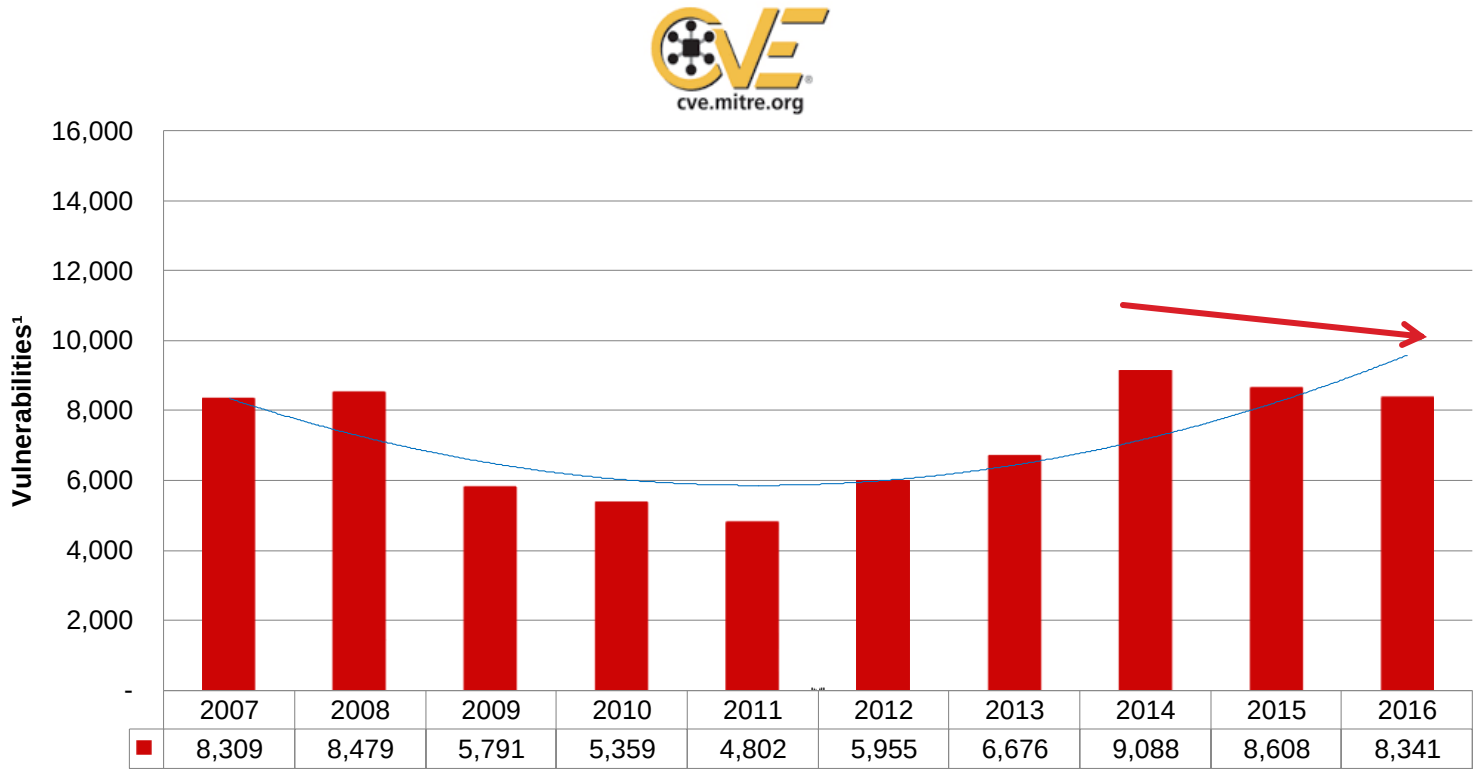
2016 is the New High Mark for Total Vulnerabilities



[1]As of January 23, 2017

VulnDB
EVERYTHING IS VULNERABLE

CVE/NVD Shows Three Year Downward Trend

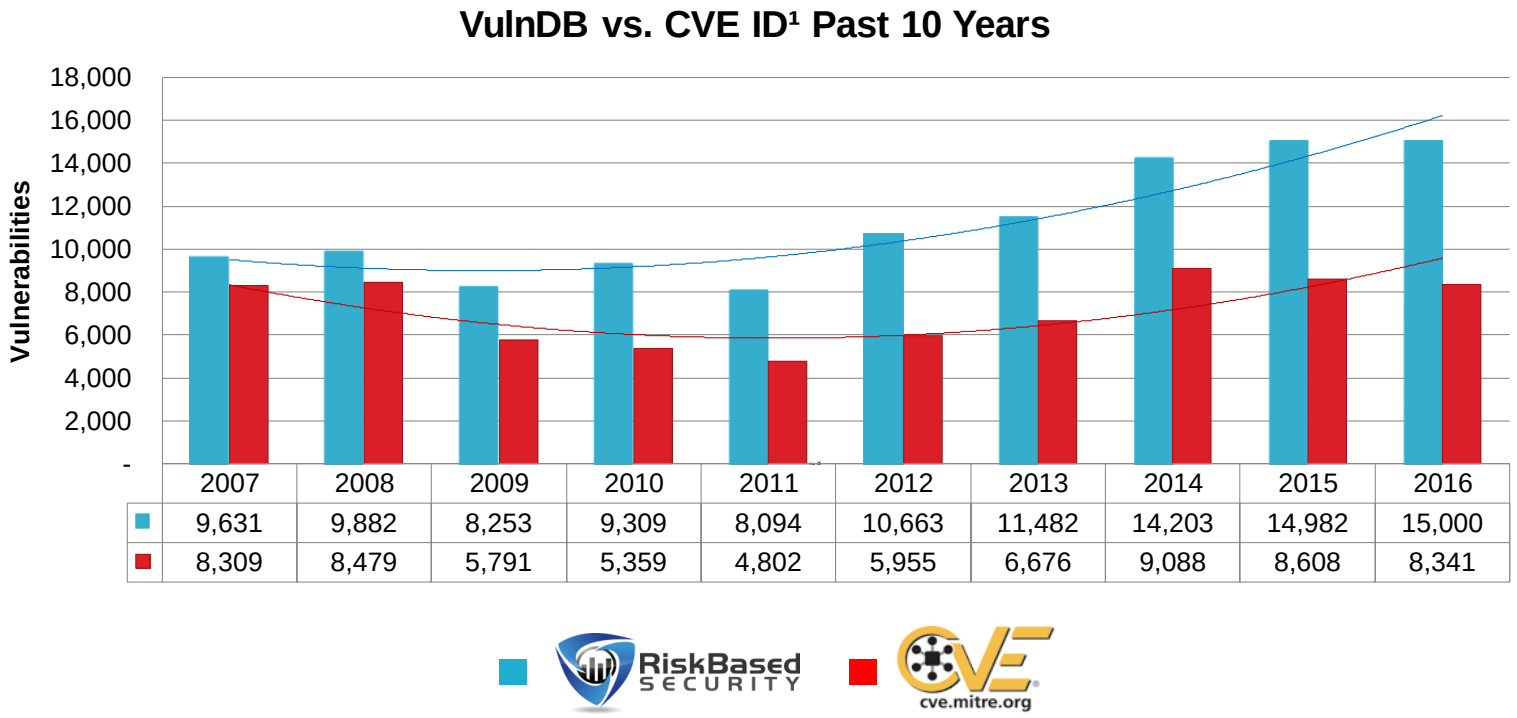


	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
■	8,309	8,479	5,791	5,359	4,802	5,955	6,676	9,088	8,608	8,341

[1]Total number of unique vulnerabilities published by CVE/NVD in each year that have an associated CVE ID.

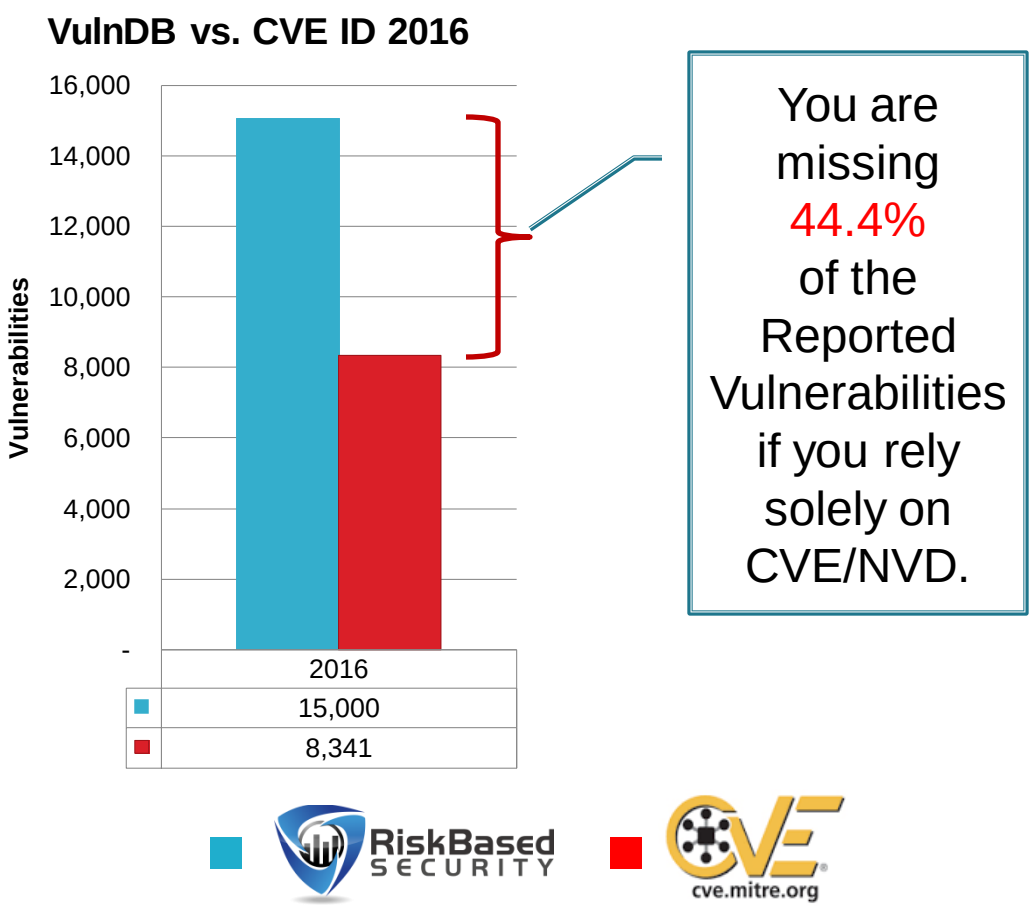
[2] 1,945 of the 2016 public vulnerabilities with CVE IDs are still marked RESERVED and missing from CVE/NVD.

CVE/NVD Published 55.6% of the 2016 Vulnerabilities Found in VulnDB

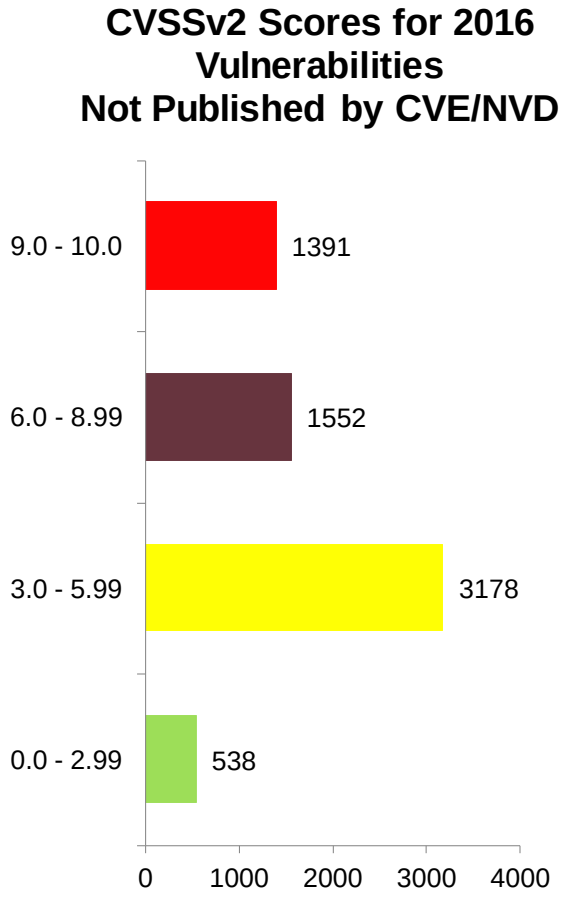


[1]Total number of unique vulnerabilities published by CVE/NVD in each year that have an associated CVE ID.

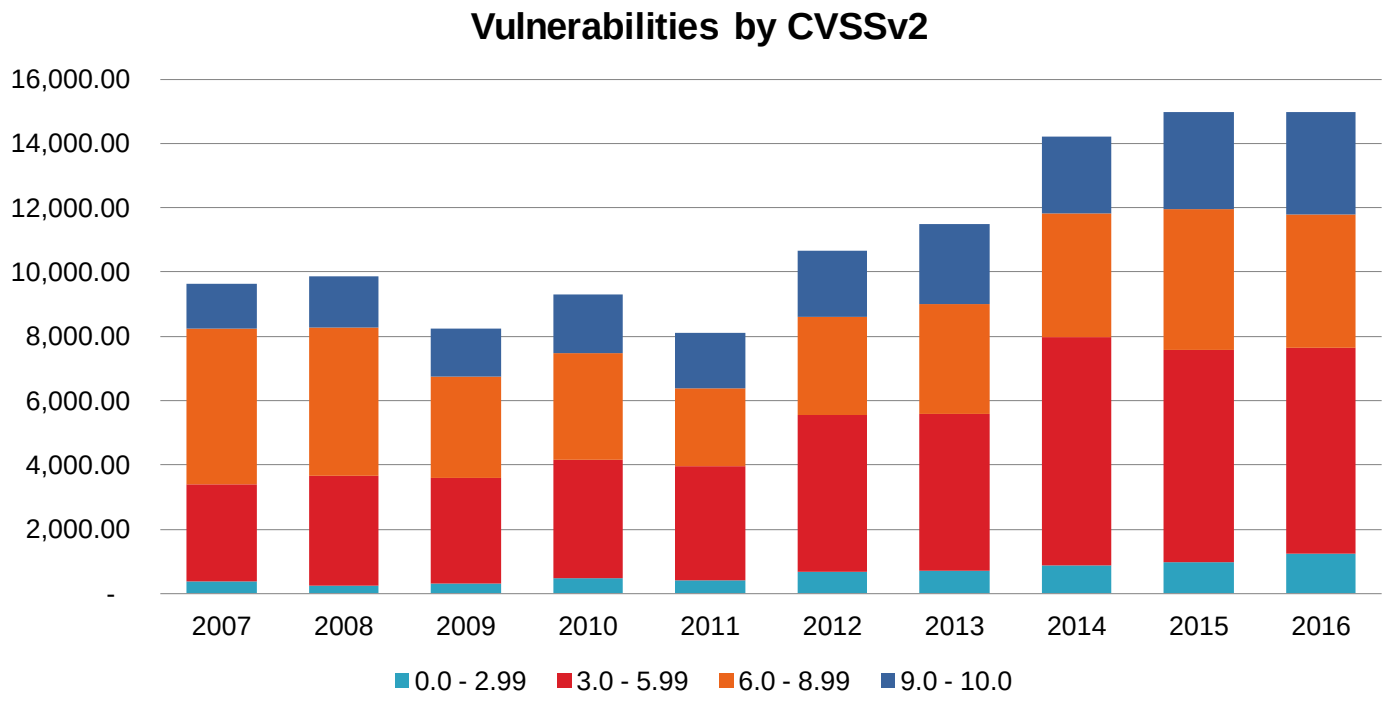
6,659 Vulnerabilities Not Found in CVE/NVD: 1,391 have Scores Above 9.0



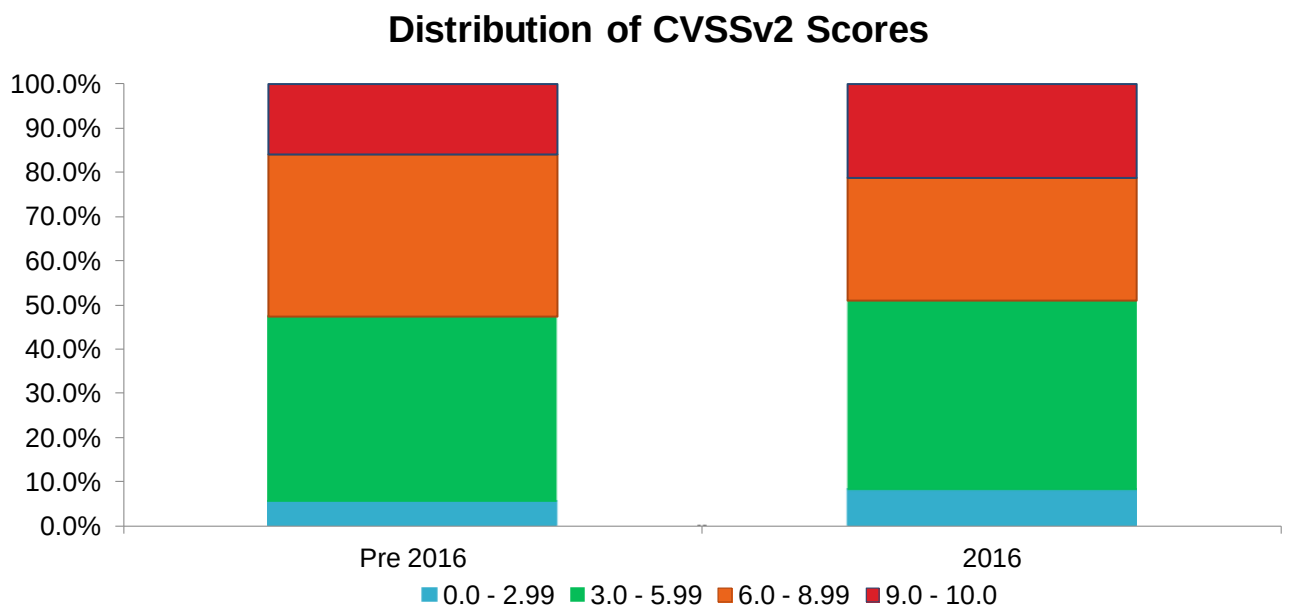
You are missing 44.4% of the Reported Vulnerabilities if you rely solely on CVE/NVD.



Both Quantity and Severity of Vulnerabilities Increasing



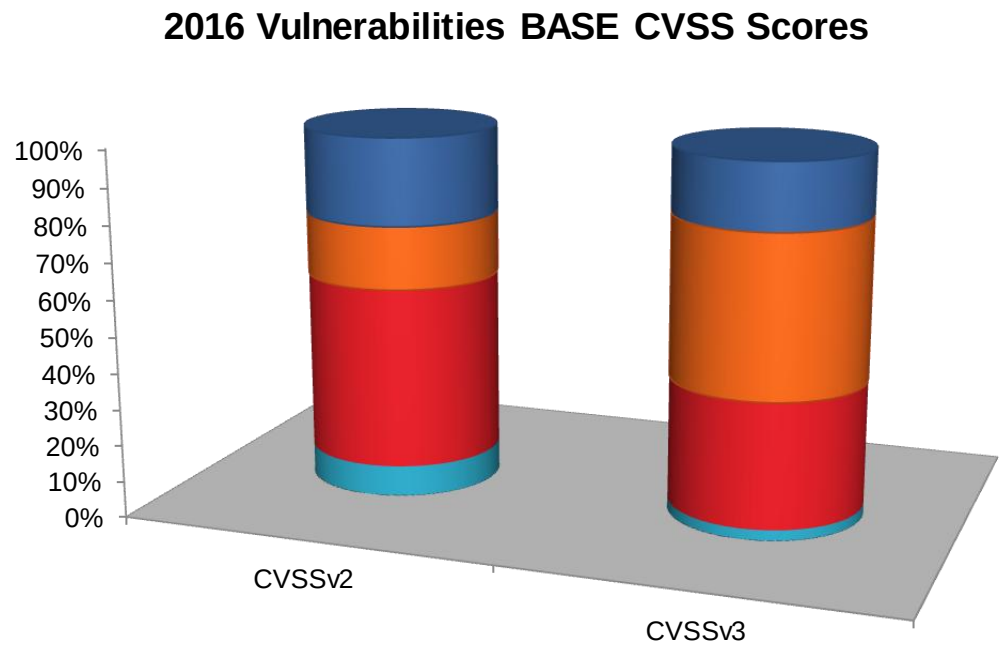
CVSSv2 Scores 9.0 and Above Account for 21.3% of all 2016 Vulnerabilities



While no one is fully happy with CVSSv2, it does provide some guidance on severity.

Note: CVSSv3 has been released and while improvements have been made, issues remain.

CVSSv2 vs. CVSSv3 BASE Scores for 2016 [As Scored by CVE/NVD]

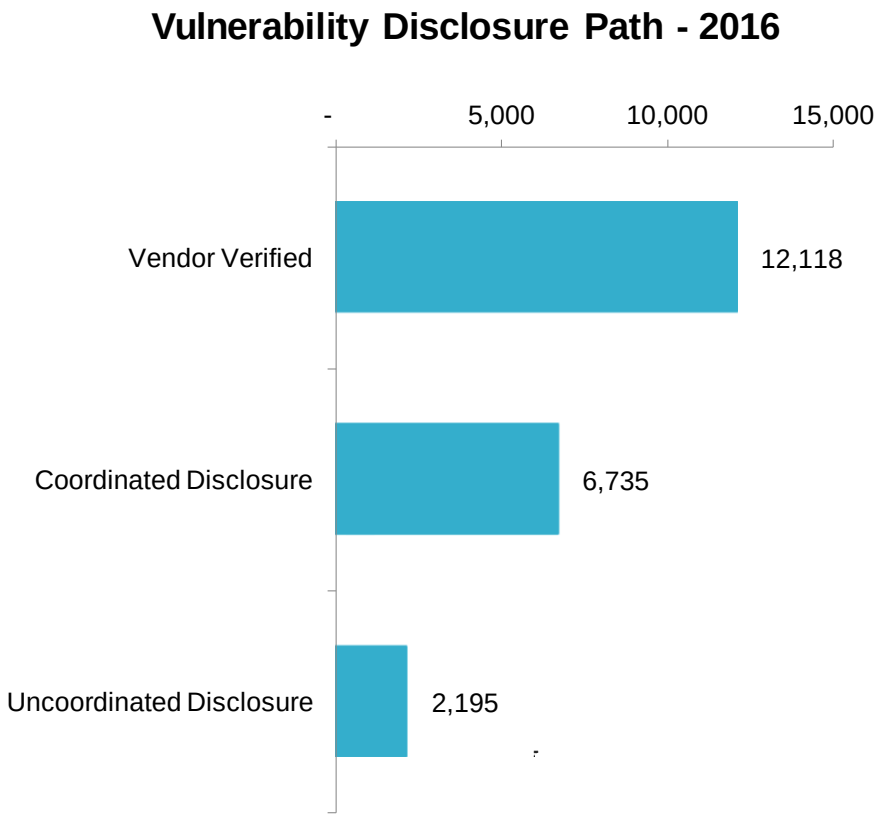


	CVSSv2	CVSSv3
9.0 - 10.0	24.1%	18.1%
6.0 - 8.99	17.4%	44.4%
3.0 - 5.99	50.0%	34.6%
0.0 - 2.99	8.5%	2.9%

V3 Impact on V2 Scores

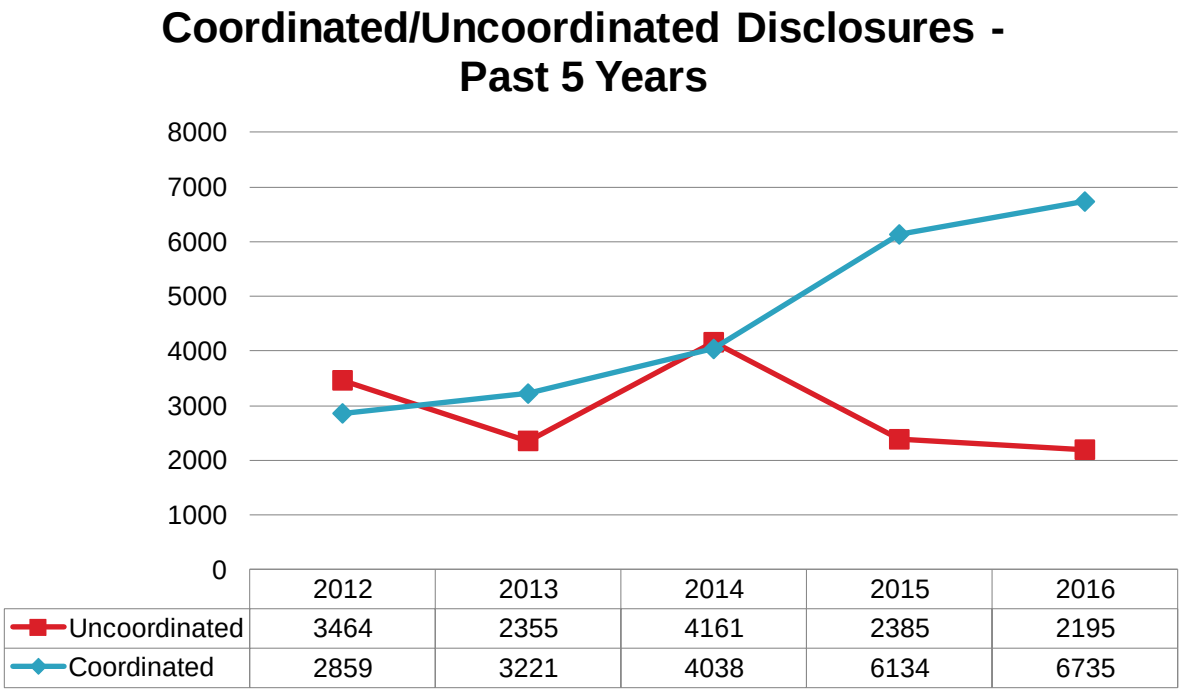
24.9% Reduction in “Critical”
155.2% Increase in “High”
30.8% Reduction in Medium”
65.9% Reduction in “Low”

80.8% of Vulnerabilities Are Verified By Vendors



VulnDB
EVERYTHING IS VULNERABLE

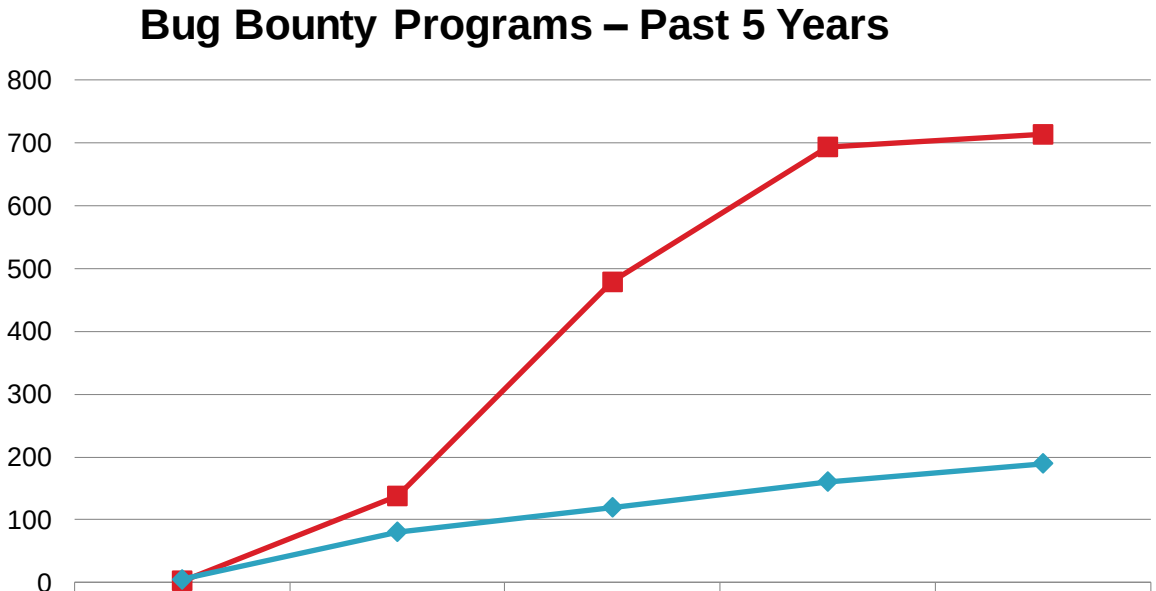
Coordinated Disclosures Outpaced Uncoordinated 3 to 1 in 2016



	2012	2013	2014	2015	2016
Uncoordinated	3464	2355	4161	2385	2195
Coordinated	2859	3221	4038	6134	6735

VulnDB
EVERYTHING IS VULNERABLE

Third Party Bug Bounty Outpaced Vendor Programs 4 to 1 in 2016

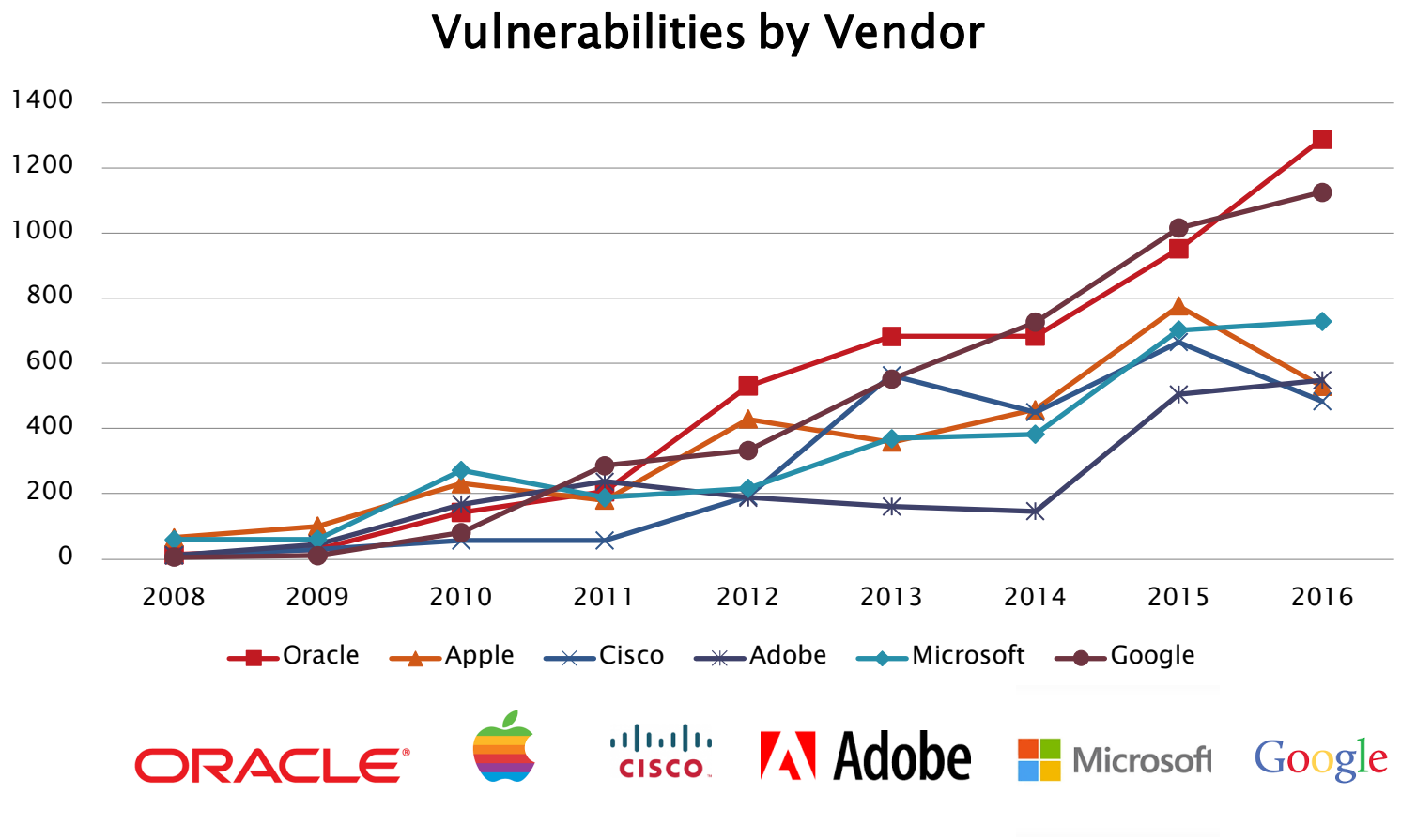


	2012	2013	2014	2015	2016
3rd Party	3	138	479	694	714
Vendor	5	81	120	161	190

[1]Based on Bug Bounty disclosures made public.

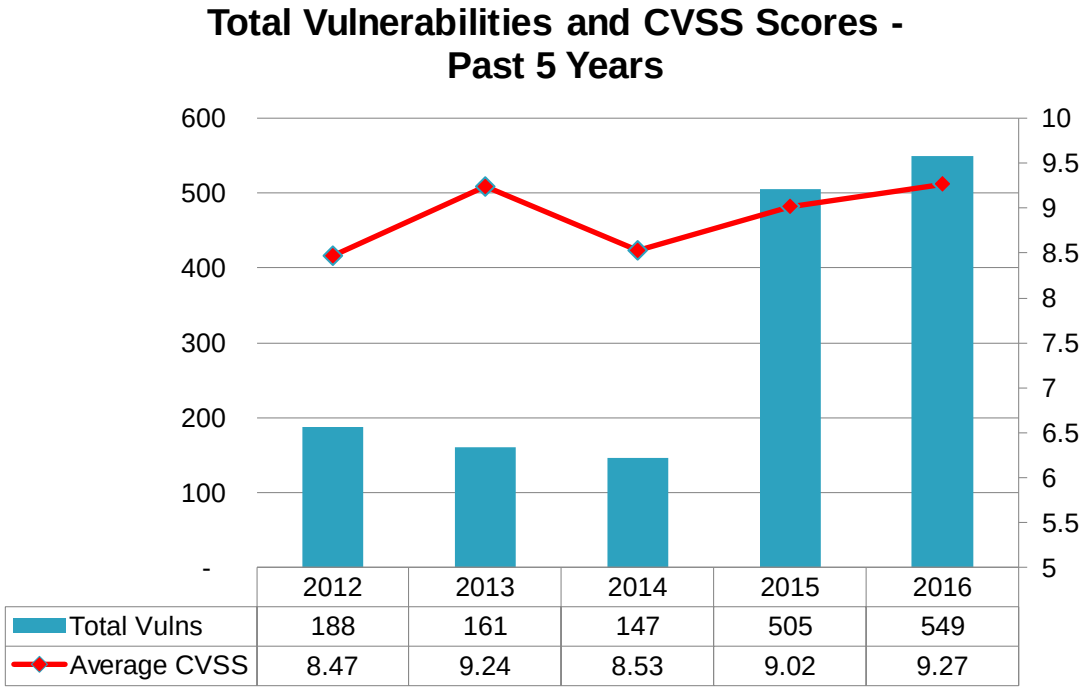
VulnDB
EVERYTHING IS VULNERABLE

Cisco and Apple Show Decrease in Number of Vulnerabilities for 2016



Adobe History – Past Five Years

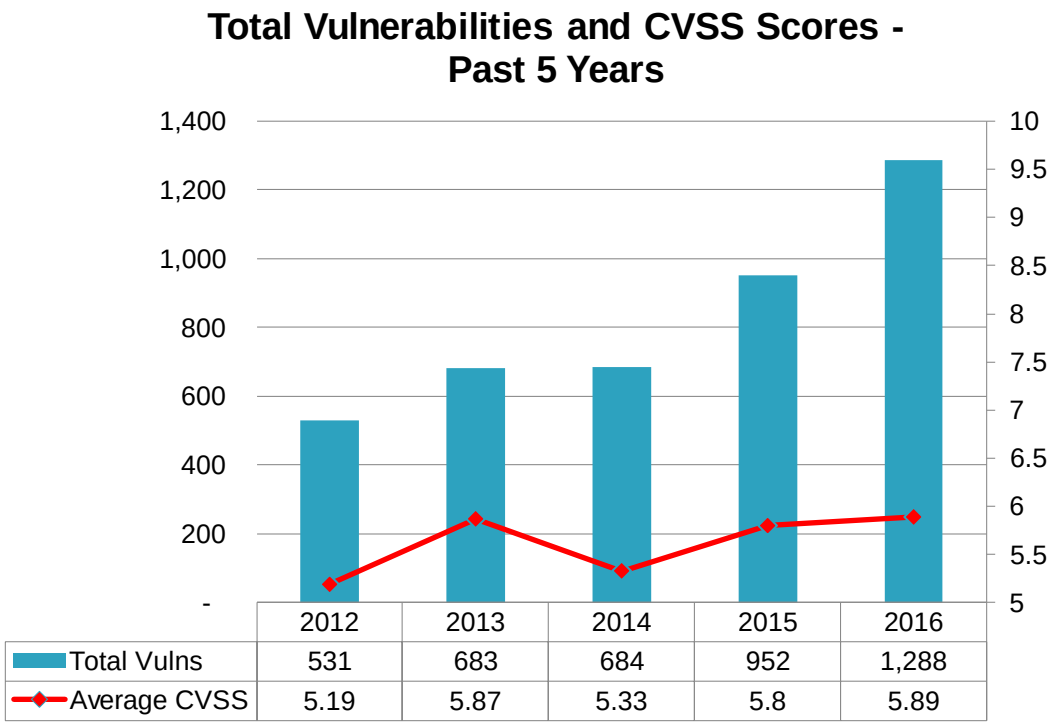
Adobe



Product Name (Top 5)	All Time Vulnerability Count
Flash Player	932
Acrobat	708
Adobe Reader	660
AIR	616
Acrobat DC	379

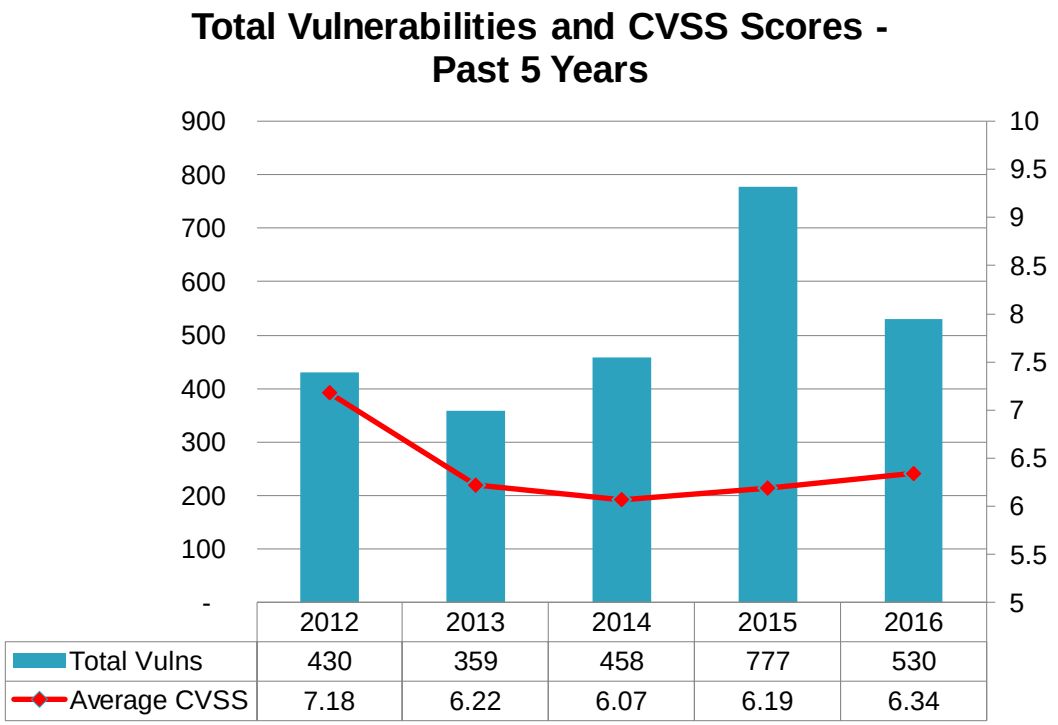
Oracle History – Past Five Years

ORACLE®



Product Name (Top 5)	All Time Vulnerability Count
Solaris	1,454
Java JRE/JDK (Java SE)	556
MySQL Server	384
E-Business Suite	361
Oracle Database Server	331

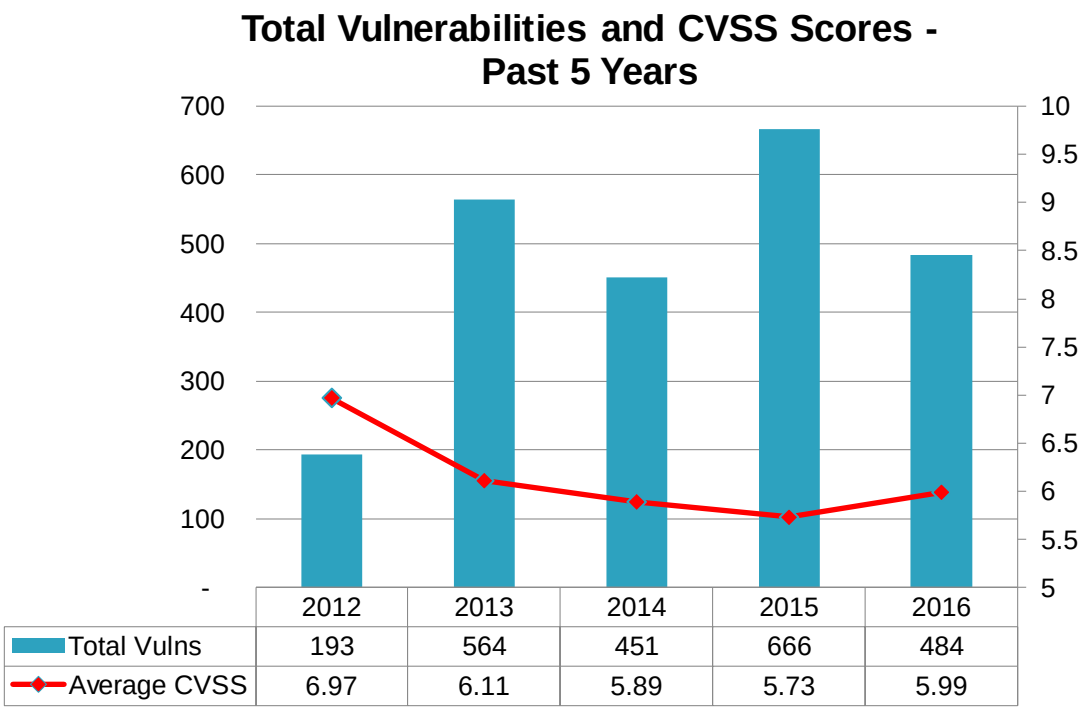
Apple History – Past Five Years



	2012	2013	2014	2015	2016
Total Vulns	430	359	458	777	530
Average CVSS	7.18	6.22	6.07	6.19	6.34

Product Name (Top 5)	All Time Vulnerability Count
Mac OS X	1,776
WebKit	1,170
Apple IOS	1,071
Safari	637
Apple TV (tvOS)	554

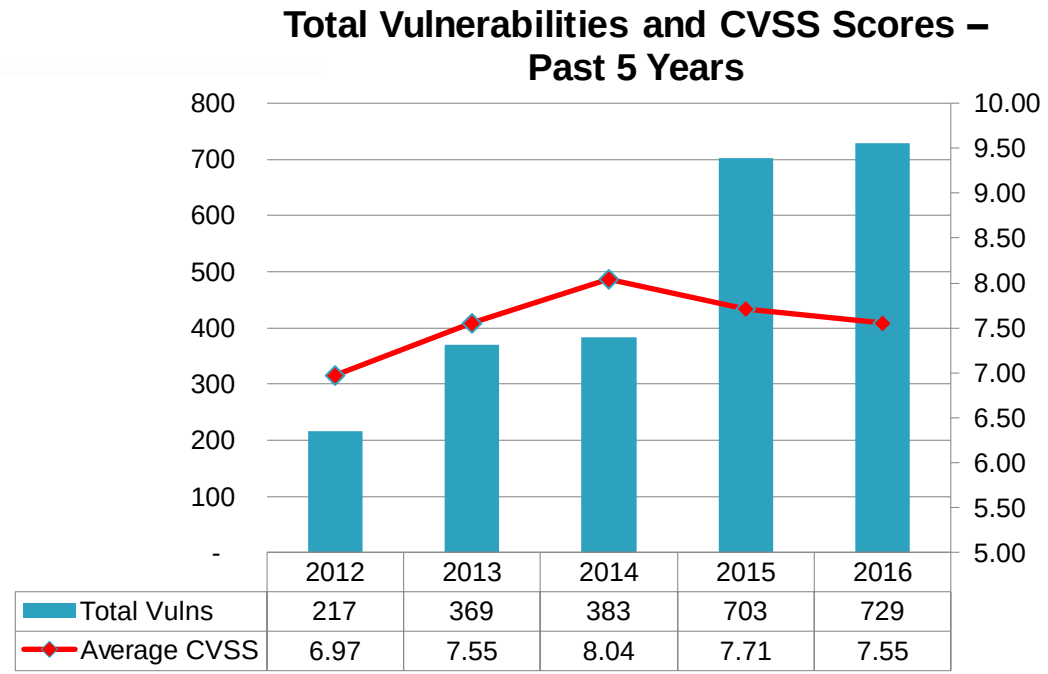
Cisco History – Past Five Years



Product Name (Top 5)	All Time Vulnerability Count
Cisco IOS	412
Firepower System (FireSIGHT)	322
Cisco IOS XE	226
Unified Communications Manager (CUCM)	210
Adaptive Security Appliance (ASA)	199

Microsoft History – Past Five Years

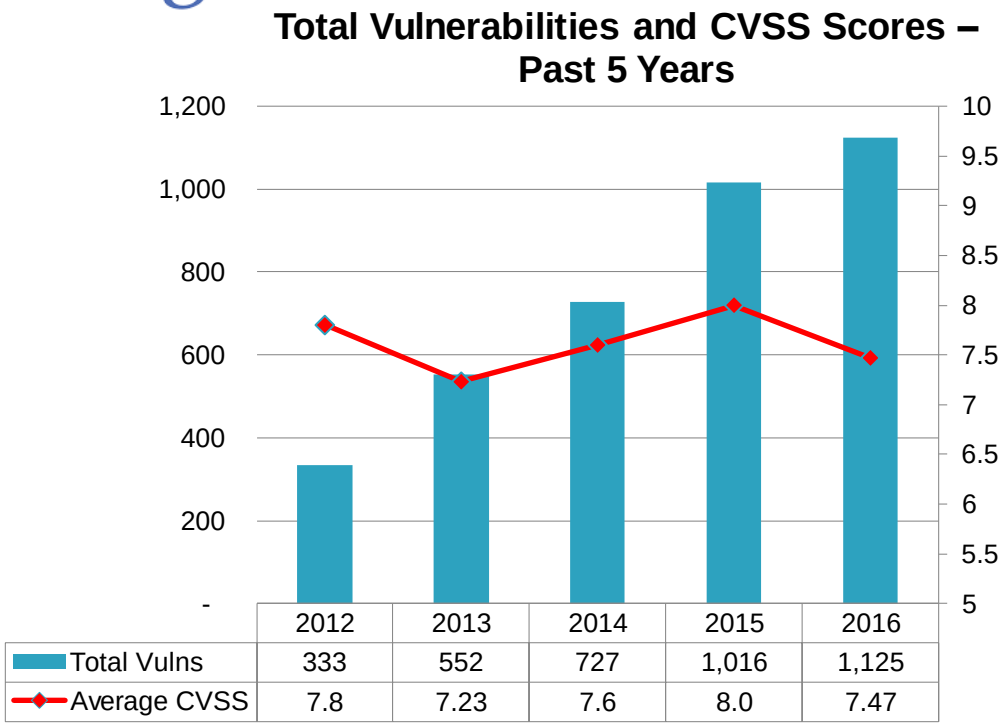
Microsoft



Product Name (Top 5)	All Time Vulnerability Count
Internet Explorer	1,261
Windows 10	705
Windows Server 2012	660
Windows 7	647
Windows Vista	621

Google History – Past Five Years

Google



Product Name (Top 5)	All Time Vulnerability Count
Chrome	2,406
Google Nexus / Pixel Devices	725
Chrome OS	613
Android	586
PDFium	300

VTEM - Vulnerability Timeline and Exposure Metrics [2016]

VulnDB's VTEM framework tracks vulnerability timelines to assist organizations with the evaluation of software vendors and products and provides insight into cost of ownership.

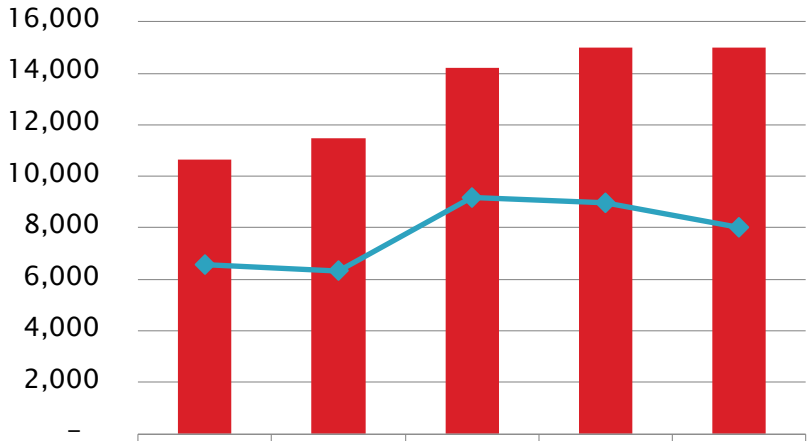
Vendor	Average Vendor Response Time (Days)	Average Time Until Patch is Available (Days)	Average Time Until an Exploit is Available (Days)
Microsoft	11	77	35
Adobe	14	78	1
Apple	9	61	9
Cisco	11	76	137
Oracle	7	78	23
Google	3	82	47

- Which vendor has the lowest cost of ownership?
- How do your vendors stack-up?

VulnDB
EVERYTHING IS VULNERABLE

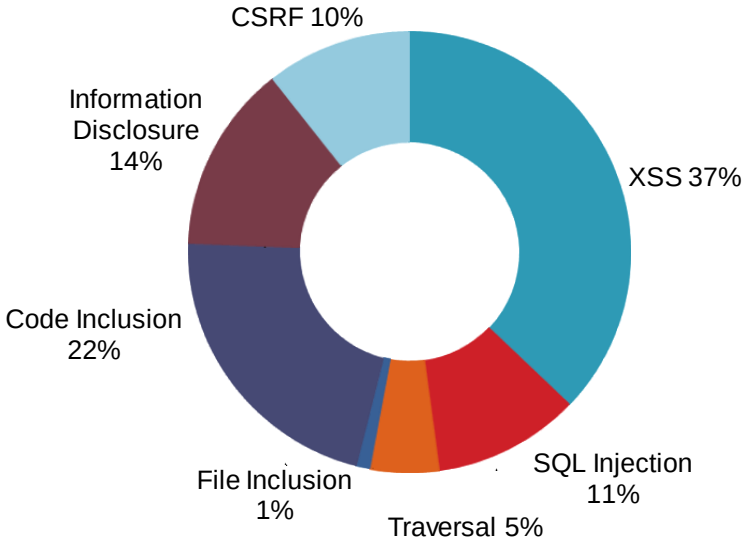
Cross-Site Scripting Tops the List of Web Related Vulnerabilities in 2016

Web Related Vulnerabilities vs. Total - Past 5 Years



	2012	2013	2014	2015	2016
Total Vulns	10,663	11,482	14,206	14,980	15,000
Web	6575	6342	9176	8972	8021

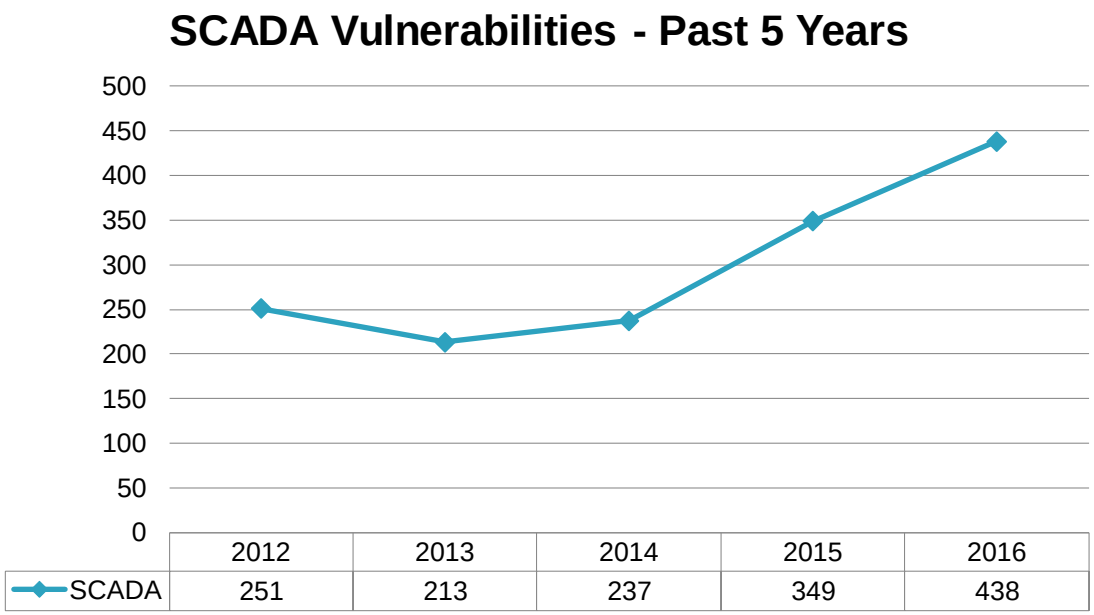
2016 Web Vulnerabilities by Type



XSS vulnerabilities have been reported and exploited since the1990s and are still prevalent in software today.

VulnDB
EVERYTHING IS VULNERABLE

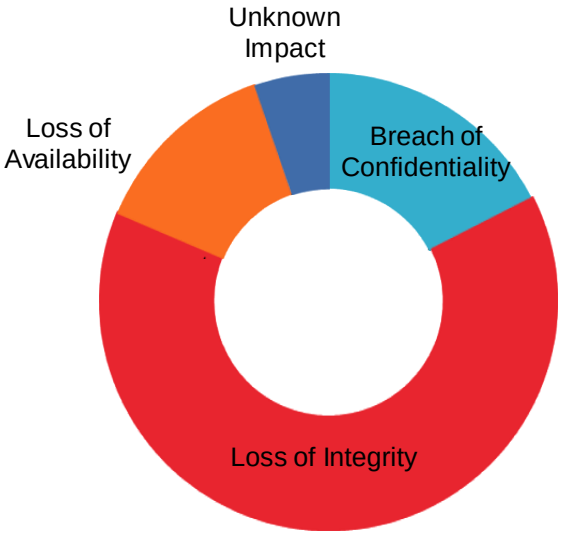
Vulnerabilities in SCADA Software Up 84.8% from 2014



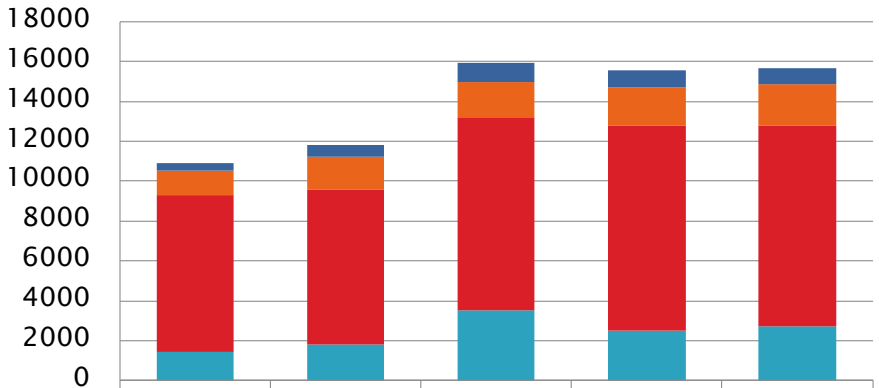
VulnDB
EVERYTHING IS VULNERABLE

Loss of Integrity Tops the List in Every Year for Past Five Years

2016 Vulnerabilities by Impact Type



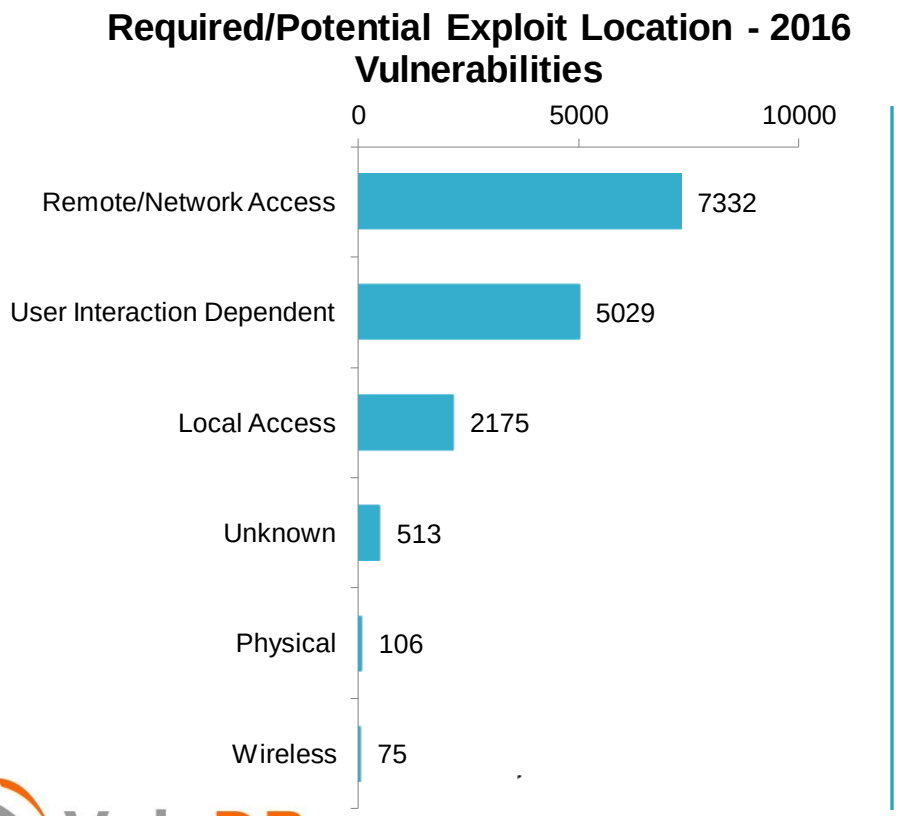
Vulnerabilities by Impact - Past 5 Years

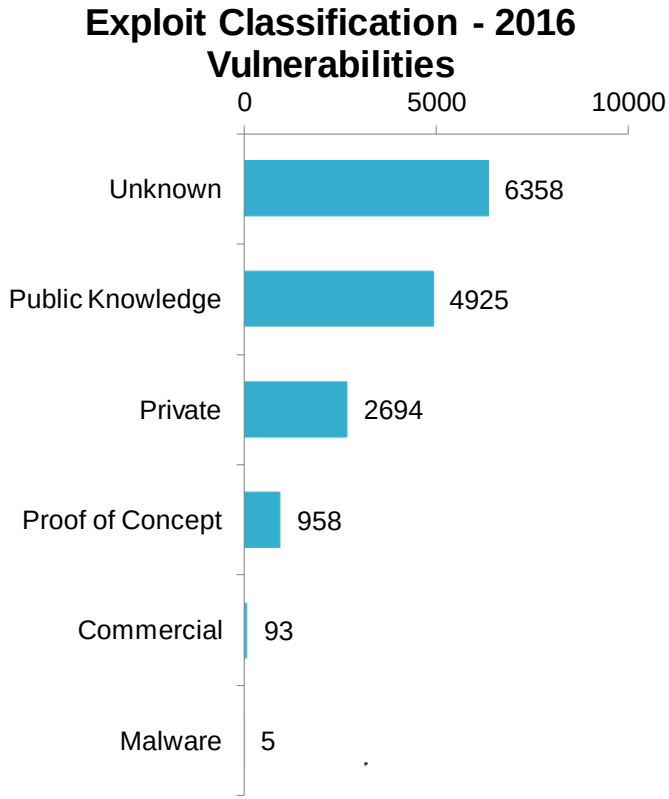


	2012	2013	2014	2015	2016
Unknown	357	578	961	845	816
Availability	1208	1698	1772	1950	2105
Integrity	7908	7755	9704	10266	10030
Confidentiality	1414	1797	3508	2491	2744

VulnDB
EVERYTHING IS VULNERABLE

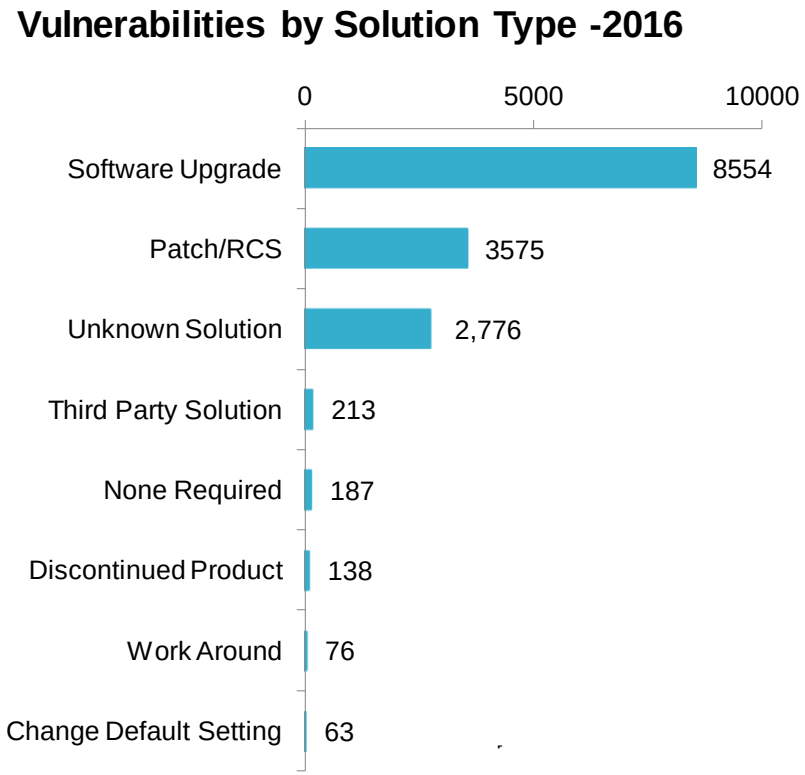
48.9% of 2016 Vulnerabilities Can Be Exploited Remotely





VulnDB
EVERYTHING IS VULNERABLE

Software Upgrade Tops the Solution List in 2016



VulnDB
EVERYTHING IS VULNERABLE

VulnDB Methodology

Vulnerability Database (VulnDB) – *The most comprehensive, highest quality and most timely vulnerability database available.*

VulnDB provides actionable intelligence about the latest in security vulnerabilities through an easy-to-use SaaS Portal, Database Export, or RESTful APIs, and/or eMail Alerting, integrating easily into vulnerability scanners, management reporting and ticketing system.

VulnDB is derived from a proprietary search engine and daily analysis of thousands of vulnerability sources. Unlike some vulnerability data base providers, Risk Based Security is constantly searching for and adding new sources.

VulnDB counts only distinct vulnerabilities. Products including a vulnerable code are not considered a unique vulnerability. To be clear, a vulnerability in a third-party library such as OpenSSL is one vulnerability. The products that use and integrate that code are not included in VulnDB counts.
https://vulndb.cyberriskanalytics.com/

VulnDB
EVERYTHING IS VULNERABLE

Data as of January 23, 2017

Risk Based Security – Cyber Risk Intelligence Experts

Cyber Risk Analytics (CRA)

Global visibility into the data breach landscape. Provides actionable intelligence about data breach types, threat vectors, exposed data types and industries most impacted through an easy-to-use SaaS Portal, Database Export, or RESTful APIs, integrating easily into security awareness programs, intelligence dashboards and vendor management systems. eMail Alerting, Breach Severity, Exposed eMail Addresses, Vendor Management, Data Breach Reports, and PreBreach Calculations. https://cyberriskanalytics.com//

YourCISO

Aimed at assisting small and medium-sized organizations that do not have security resources on staff by providing ready access to security intelligence and the right expertise on an as-needed basis at affordable prices. Data Breach Reports, Awareness Training, Policy Templates, Security Program Health Check and Consultant Scheduling Tool. https://yourciso.com//

No Warranty

Risk Based Security, Inc. makes this report available on an "As-is" basis and offers no warranty as to its accuracy, completeness or that it includes all the latest vulnerabilities. The information contained in this report is general in nature and should not be used to address specific security issues. Opinions and conclusions presented reflect judgment at the time of publication and are subject to change without notice. Any use of the information contained in this report is solely at the risk of the user. Risk Based Security, Inc. assumes no responsibility for errors, omissions, or damages resulting from the use of or reliance on the information herein. If you have specific security concerns please contact Risk Based Security, Inc. for more detailed vulnerability analysis and security consulting services.