Software Security

CORSO DI SICUREZZA DELLE RETI E DEI SISTEMI SOFTWARE
AA 2017/18

ING. ANTONIO PIROZZI

#cat /dev/user

- Director of Malware Research Lab at CSE CybSec Enterprise spa
- Senior Researcher and co-founder of Iswatlab
- Exam item writer for EC-Council
- Lecturer for 2 level Master in CyberSecurity at LinkCampus University
- More than 12 Infosec certification
- Hack3r of course!

Outline

- Fundamentals
- Software Vulnerabilities and Exploits
- Vulnerability Disclosure
- Vulnerability Assessment & Penetration Test
- Risk Evaluation
- Risk Assessment : Qualitative vs Quantitative
- CVSS
- VA&PT hands-on

“I’m not interested in How system works, but In How they fails”. B. Schneier

Software Security Fundamentals
(*good sw engineering*)

- **Functional requirements**
  - Software must do what is expected to do
- **Non-functional requirements (horizontal requirement)**
  - Security
  - Safety
- There are no perfect softwares
- There are only things that are secure "*enough*"..

Threat and Risk

- Threat' is a function of the enemy's capability and intent to conduct attacks, whereas 'risk' is a function of the probability that your organisation will be involved in an attack. Cit. Threat and Risk: What's the Difference **David Strachan-Morris**
- 'threat' = capability x intent

Threats vs Security Requirements

- **Information Disclosure**
  - Confidentiality
- **Tampering**
  - Integrity
- **Denial of Service**
  - Availability
- **Spoofing**
  - Authentication
- **Unauthorized Access**
  - Access Control

Software Vulnerabilities

- Software is designed (should) to meet requirements
- A **software bug** is un *unmet specification*, a failure in meet the requirements.
- If a bug is related to a security requirement, it is a Software Vulnerability
  - Vulnerability is a subset of bug
- A Vulnerability is a bug the has a reflect on constraints of CIA (Confidentiality, Integrity, Availability)
  - Weakness or gap
- **Exploit** is a set of instructions for abusing a sw vulnerability in order to cause unintended or unanticipated behavior.

Vulnerability Disclosure

- Full Disclosure
- Responsible Disclosure
- Bug Bounty Programs

Vulnerability Disclosure

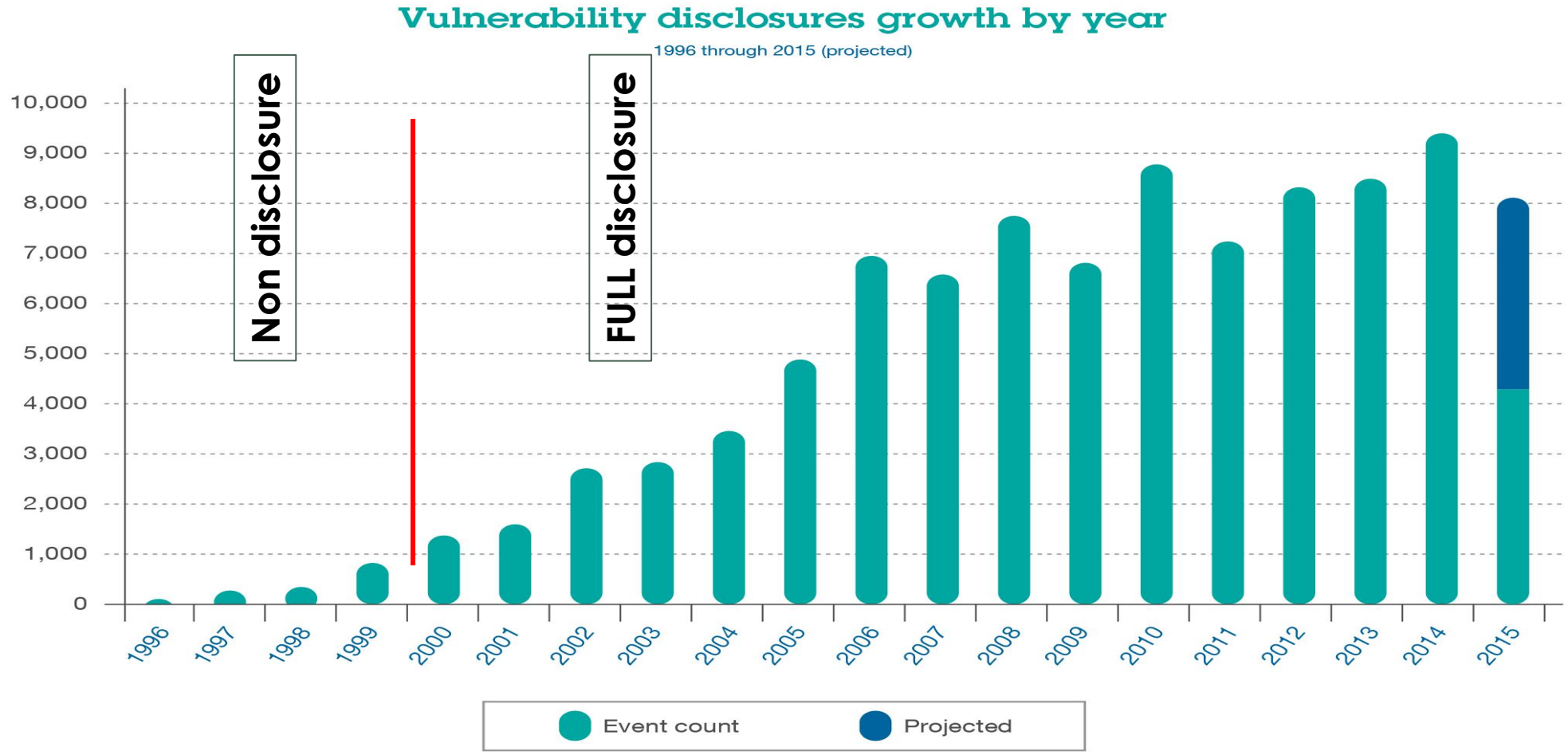
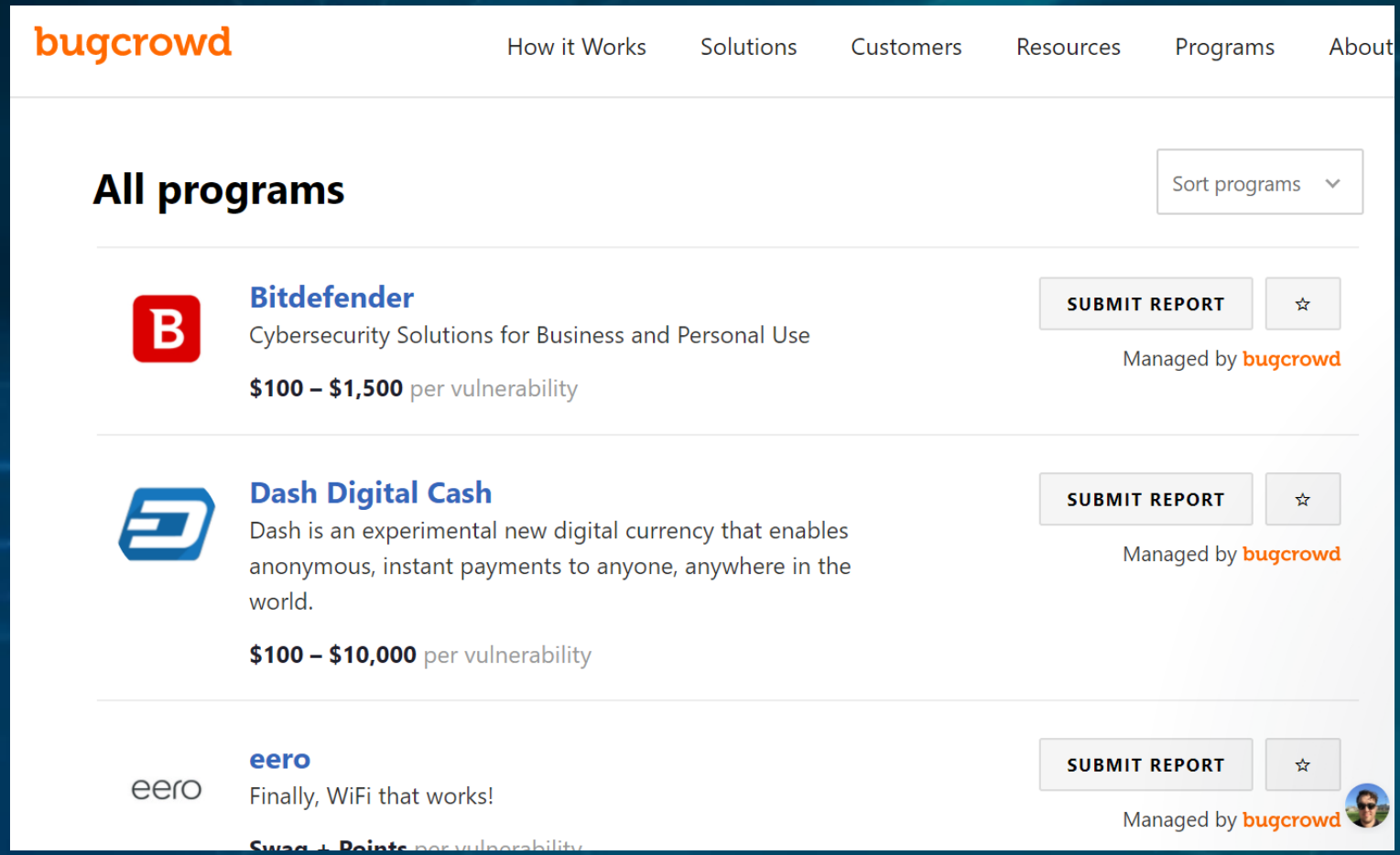


Figure 4. Vulnerability disclosures growth by year, 1996 through 2015 (projected)

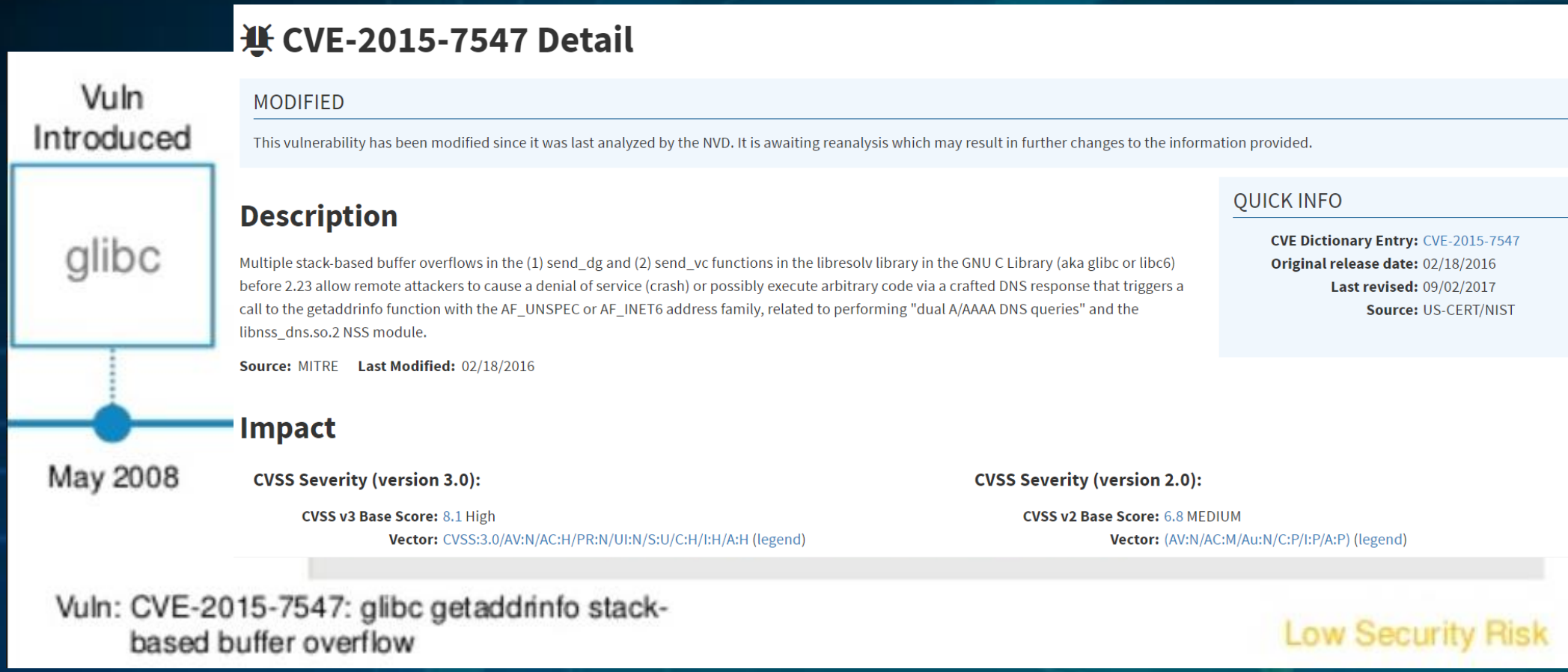
Source: IBM X-Force® Research and Development

Responsible Disclosure: Bug Bounty

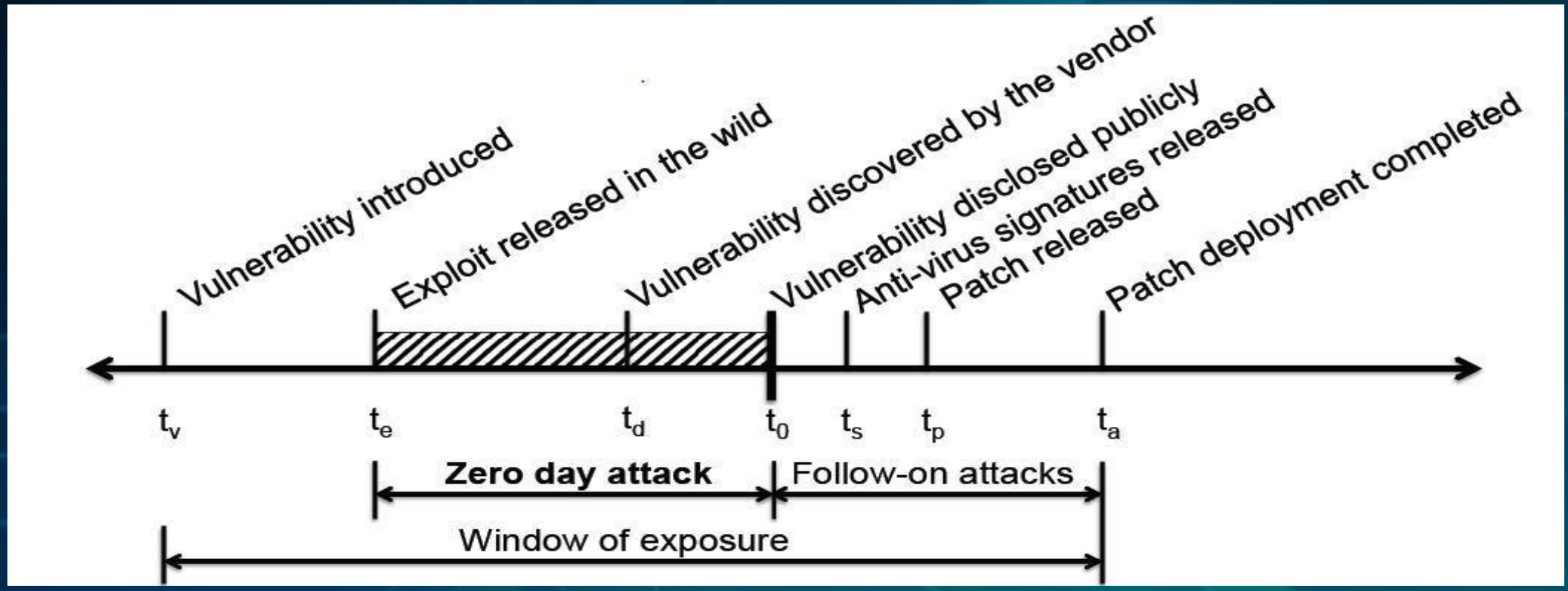


Responsible Disclosure: Bug Bounty

Knowledge is the key



Vulnerability Disclosure Timeline

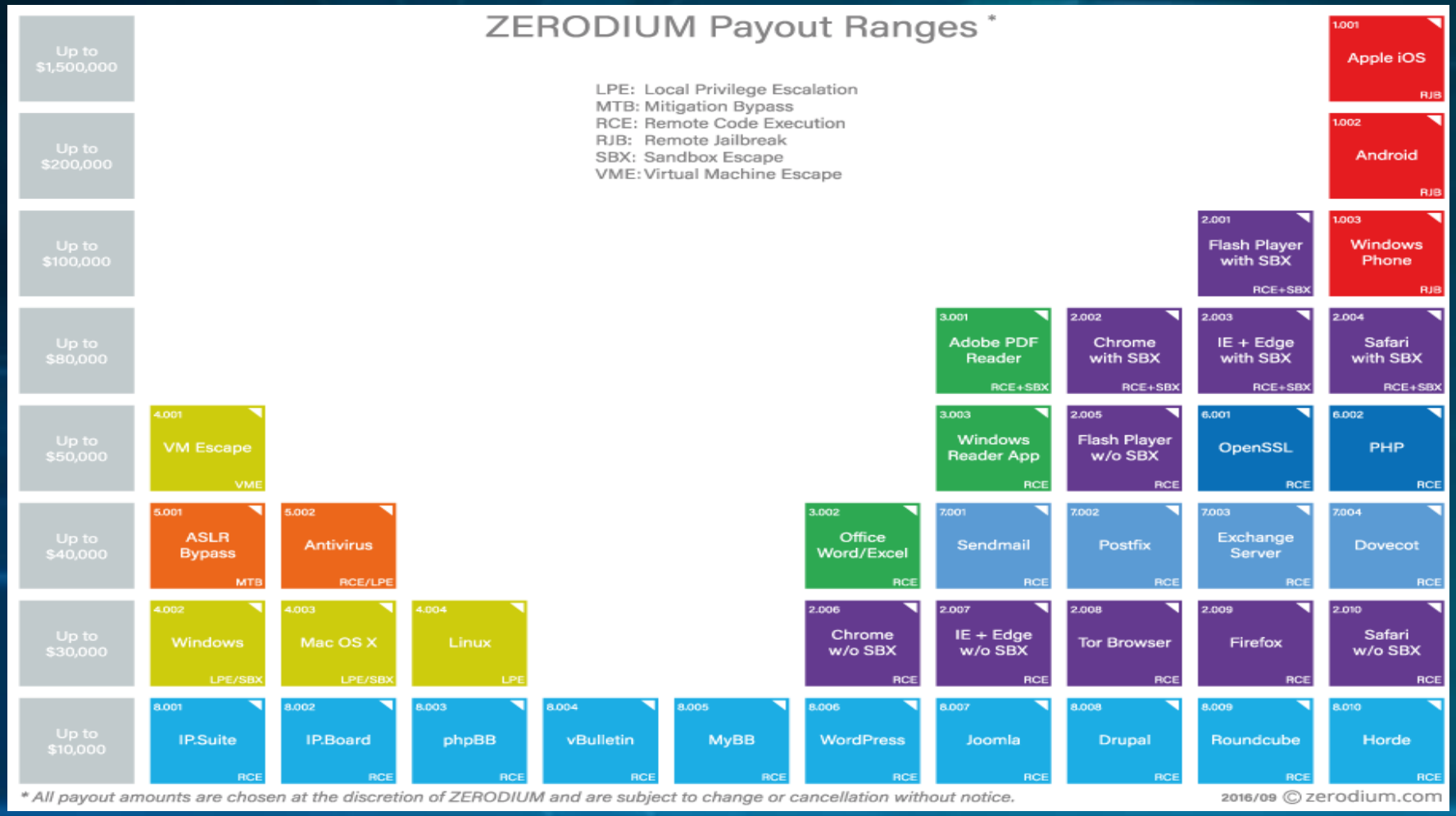


Responsible Disclosure

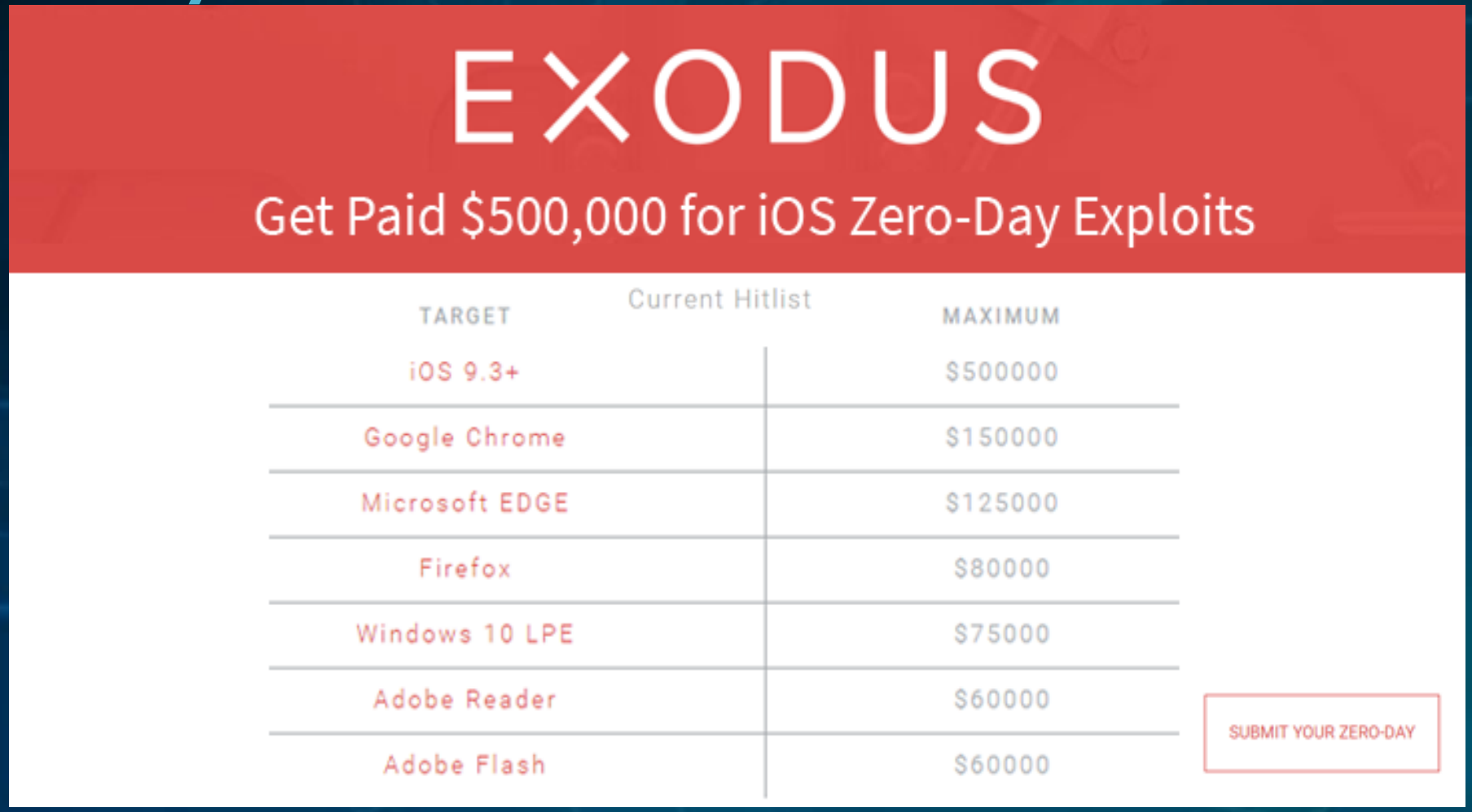
- All stakeholders agree to allow a period of time for the vulnerability to be patched before publishing the details.

- Dan Kaminsky discovery of DNS cache poisoning, 5 months
- MD5 collision attack that shows how to create false CA certificates, 1 week
- Starbucks gift card double-spending/race condition to create free extra credits, 10 days (Egor Homakov)[7]

0-day Market


ZERODIUM Payout Ranges *
LPE: Local Privilege Escalation
MTB: Mitigation Bypass
RCE: Remote Code Execution
RJB: Remote Jailbreak
SBX: Sandbox Escape
VME: Virtual Machine Escape
Up to $1,500,000
Up to $200,000
Up to $100,000
Up to $80,000
Up to $50,000
Up to $40,000
Up to $30,000
Up to $10,000
1.001 Apple iOS RJB
1.002 Android RJB
2.001 Flash Player with SBX RCE+SBX
1.003 Windows Phone RJB
3.001 Adobe PDF Reader RCE+SBX
2.002 Chrome with SBX RCE+SBX
2.003 IE + Edge with SBX RCE+SBX
2.004 Safari with SBX RCE+SBX
4.001 VM Escape VME
3.003 Windows Reader App RCE
2.005 Flash Player w/o SBX RCE
6.001 OpenSSL RCE
6.002 PHP RCE
5.001 ASLR Bypass MTB
5.002 Antivirus RCE/LPE
3.002 Office Word/Excel RCE
7.001 Sendmail RCE
7.002 Postfix RCE
7.003 Exchange Server RCE
7.004 Dovecot RCE
4.002 Windows LPE/SBX
4.003 Mac OS X LPE/SBX
4.004 Linux LPE
2.006 Chrome w/o SBX RCE
2.007 IE + Edge w/o SBX RCE
2.008 Tor Browser RCE
2.009 Firefox RCE
2.010 Safari w/o SBX RCE
8.001 IP.Suite RCE
8.002 IP.Board RCE
8.003 phpBB RCE
8.004 vBulletin RCE
8.005 MyBB RCE
8.006 WordPress RCE
8.007 Joomla RCE
8.008 Drupal RCE
8.009 Roundcube RCE
8.010 Horde RCE
* All payout amounts are chosen at the discretion of ZERODIUM and are subject to change or cancellation without notice.
2016/09 © zerodium.com

0-day Market


EXODUS
Get Paid $500,000 for iOS Zero-Day Exploits
Current Hitlist
TARGET
MAXIMUM
iOS 9.3+
$500000
Google Chrome
$150000
Microsoft EDGE
$125000
Firefox
$80000
Windows 10 LPE
$75000
Adobe Reader
$60000
Adobe Flash
$60000
SUBMIT YOUR ZERO-DAY

Cyber Warfare

- **Duqu2** uses a kernel mode exploit for CVE-2015-2360 to load its kernel mode component.
- **Turla** uses 2 exploit for CVE-2013-5065 and CVE-2013-3346
- **Stuxnet** use 4 exploit for CVE-2010-2568, CVE-2010-2729, CVE-2008-4250, CVE-2010-2722 (American-Israeli Cyber Weapon)
- **BlackEnergy** use a memory corruption vulnerability CVE-2014-1761and an RCE vulnerability CVE-2014-4114

Vulnerability Assessment & Penetration Test

- A Vulnerability Assessment is the way to find as many flaws as possible and make a prioritized list of remediation items.
  - List Oriented
  - Don't differentiate between flaws that can be exploited to cause damage and those that cannot.
- A Penetration Test is an intrusive test, simulating real threat scenario and it is designed to evaluate also the defense measures in place.
  - Goal oriented
  - A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system
- Often combined to achieve more cohmprensive security analysis

Vulnerability Assessment & Penetration Test

- Vulnerability Assessment: Find every flaws in a system
- Vulnerability Assessment is not Risk Assessment!
- Penetration Test: Evaluate how damaging a flaw could be in real attack.
- VAPT provides a detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks

RISK FORMULA

- Greater is the Threat..
- ..more likely the system could be attacked

- More vulnerable is the system..
- ..greater is the probability that the system could be compromised

Risk Evaluation

- There are several options to address the risk:
- Accept
- Avoid
- Transfer
- Mitigate

Risk Costs

- Implemetation
- Additional support
- Training
- Reduction in operational effectiveness

- All these costs need to be balanced
- Without true sense of control's cost over time the company can't make risk decisions

Risk Evaluation

- Don’t just rely on vulnerability counts to understand your exposure to threats and exploits.
- To evaluate the Risk we need to identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
- Risk assessment is one of the most critical parts of risk management, and also one of the most complex – affected by human, technical, and administrative issuesReduces chances of a security breach/stolen information, as it allows companies to react quicker to potential threats
- improving organizational security posture

Risk Evaluation for compliance Requirements

- **PCI DSS v3.0 Req. 11.2.1:** quarterly internal scans and rescans until all 'high risk' vulnerabilities are resolved.
- **PCI DSS v3.0 Req. 11.2.2 :** requires quarterly external scans and rescans until no vulnerabilities exist that are scored 4.0 or higher by the CVSS.
- **PCI DSS v3.0 Req. 11.2.3 :** requires internal and external scanning, and rescanning, after any significant change to the network.

Qualitative vs Quantitative Risk Evaluation

- **Qualitative risk evaluation:**
- how **low**, **medium** or **high** a threat is.
- give understanding to the weight (qualitative) of a particular compromise to the reputation of a business

- **Quantitative risk evaluation:**
- Provide more accurate reflection of an organization's risk and their potential impact.
- maps a cost, a monetary loss, to a particular risk exposure

Qualitative vs Quantitative Risk Evaluation

- **Qualitative risk assessment:**
- Higly biased
- Easy and quick to perform (99% of the companies do)
- qualitative assessment useful only in the local context where it is performed

		Impact		
		Low	**Medium**	**High**
Probability	**Low**	Low Risk	Low Risk	Medium Risk
	Medium	Low Risk	Medium Risk	High Risk
	High	Medium Risk	High Risk	High Risk

Qualitative vs Quantitative Risk Evaluation

- **Quantitative risk assessment:**
- focuses on factual and measurable data, and highly mathematical and computational bases
- **SLE (Single Loss Expectancy):** money expected to be lost if the incident occurs one time.
- **ARO (Annual Rate of Occurrence):** how many times in a one-year interval the incident is expected to occur.
- **ALE (Annual Loss Expectancy):** money expected to be lost in one year considering SLE and ARO (ALE = SLE * ARO). For quantitative risk assessment, this is the risk value.

Risk Management strategy

Key aspects:

- **Assess risk and determine needs**
- **Include a total stakeholder perspective.**
- **Designate a central group of employees**
- **Implement appropriate policies and related controls**
- **Monitor and evaluate policy and control effectiveness.**

Common Vulnerability Scoring System

- "The *Common Vulnerability Scoring System (CVSS)* provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measuremen" NIST

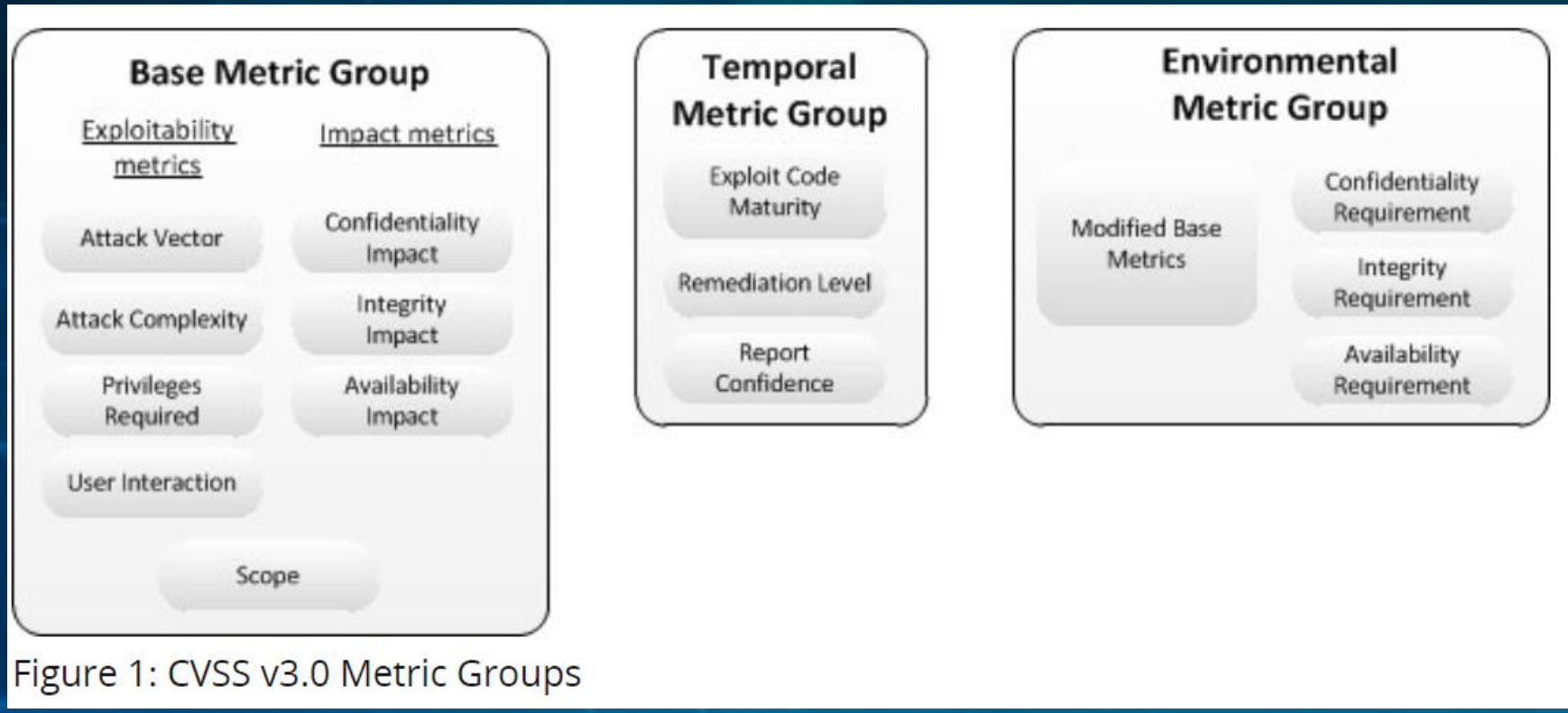
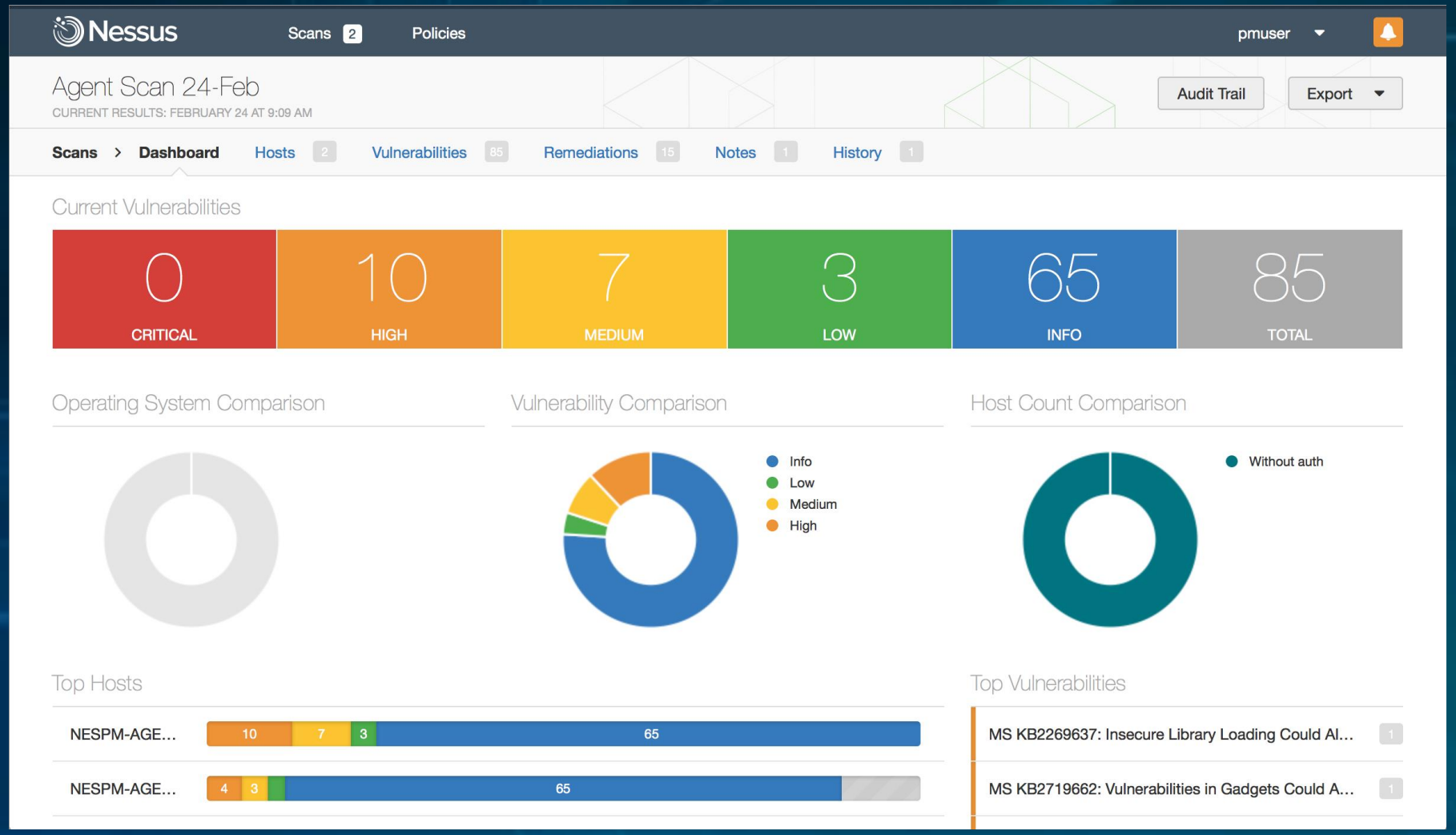


Figure 1: CVSS v3.0 Metric Groups

NESSUS DEMO


Nessus
Scans 2
Policies
pmuser
Agent Scan 24-Feb
CURRENT RESULTS: FEBRUARY 24 AT 9:09 AM
Audit Trail
Export
Scans
Dashboard
Hosts 2
Vulnerabilities 85
Remediations 15
Notes 1
History 1
Current Vulnerabilities
0 CRITICAL
10 HIGH
7 MEDIUM
3 LOW
65 INFO
85 TOTAL
Operating System Comparison
Vulnerability Comparison
Info
Low
Medium
High
Host Count Comparison
Without auth
Top Hosts
NESPM-AGE... 10 7 3 65
NESPM-AGE... 4 3 65
Top Vulnerabilities
MS KB2269637: Insecure Library Loading Could Al... 1
MS KB2719662: Vulnerabilities in Gadgets Could A... 1

Acunetix Web VS DEMO