The Cyber Exposure Company

Risk-based Vulnerability Management
Most VM programs are stale and generally viewed as either ineffective or broken!
“There is no such thing as "being secure" there's just operating at an acceptable level of risk.”
The Four Key Questions

Where are we exposed?

What should we focus on first?

How are we reducing exposure over time?

How do we compare to our peers?
Figure 2. Number of Vulnerabilities During The Past Decade

Number of Vulnerabilities Exploited During the Past Decade

Number of Vulnerabilities

- Confirmed Exploit
- No Confirmed Exploit

Source: IBM X-Force/Analysis Gartner (June 2018)

Gartner Market Guide for Vulnerability Assessment, Craig Lawson, Prateek Bhajanka, June 19, 2018
## TOP 10 VULNERABILITIES USED BY CYBERCRIMINALS IN 2018

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVSSv2 Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2018-8174</td>
<td>7.6</td>
</tr>
<tr>
<td>CVE-2018-4878</td>
<td>7.5</td>
</tr>
<tr>
<td>CVE-2017-11882</td>
<td><strong>9.3</strong></td>
</tr>
<tr>
<td>CVE-2017-8750</td>
<td>7.6</td>
</tr>
<tr>
<td>CVE-2017-0199</td>
<td><strong>9.3</strong></td>
</tr>
<tr>
<td>CVE-2016-0189</td>
<td>7.6</td>
</tr>
<tr>
<td>CVE-2017-8570</td>
<td><strong>9.3</strong></td>
</tr>
<tr>
<td>CVE-2018-8373</td>
<td>7.6</td>
</tr>
<tr>
<td>CVE-2012-0158</td>
<td><strong>9.3</strong></td>
</tr>
<tr>
<td>CVE-2015-1805</td>
<td>7.2</td>
</tr>
</tbody>
</table>

Of the top 10 Only 4 have “Critical” CVSS Score

March 19, 2019
17,313*

VULNERABILITIES DISCLOSED IN 2019

59% of vulnerabilities discovered in environments are CVSS 7+

15% of vulnerabilities disclosed in 2017 were CVSS 9+

7% of vulnerabilities had an exploit available

*National Vulnerability Database
"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want know, instead, is the risk a vulnerability or flaw poses to them, or how quickly they should respond to a vulnerability."
WHAT’S THE MISSING INGREDIENT?
TERMINOLOGY

• **Predictive Prioritization:**
  The *process* of re-prioritizing vulnerabilities based on the probability they will be leveraged in an attack.

• **Vulnerability Priority Rating (VPR):**
  The *output* of the Predictive Prioritization process. VPR is the number that indicates the remediation priority (0 through 10, with 10 being the highest severity) of an individual vulnerability.
A DATA SCIENCE APPROACH
UNDERSTANDING THE MODEL

150 different aspects in 7 groups

- Past threat pattern
- CVSS
- NVD
- Past hostility
- Vulnerable software
- Exploit code
- Past threat source

Over 140,000 vulnerabilities tracked
Forecasts probability of exploit in near term future
Updated daily
SOME OF WHAT’S IN THE MODEL

- CVE Age
- No. Words in NVD Description
- Days Since NVD Last Modified
- Number of References
- CVSS v3 Base Score
- CVSS v3 Exploitability Score
- CVSS v3 Impact Score
- Total Affected Software
- CWE

- Distinct days with cyber exploits
- Days since last cyber exploit
- Total cyber exploit events
- Days since first cyber exploit
- Days since last cyber attack

- Days since last ExploitDB entry
- Days since first ExploitDB entry
- Days since last Exploit tool entry
- Total ExploitDB entries
- Total Exploit tool entries
VPR Framework

VPR Framework: How does it Work?

CVSS v3

- Impact Score
- Scope
- Exploitability Score
- Exploit Code Maturity

VPR

- Impact Score
- Scope
- Threat Score

Past threat patterns
Past threat sources
Vulnerability metrics
Vulnerability meta data
Past hostility
Affected vendor
Exploit availability using threat intelligence data

Base Score
VPR vs CVSS scores

• VPR score is dynamic and reflects threat intelligence collected on a daily basis

• VPR score is provided weeks before a CVSS score is made public

• Often time-lag between when a CVE is published and when a CVSS score is derived
VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE

Linux Kernel Flaw
Linux Kernel Flaw

 CVE is published on NVD on Sept 19th

“In the wild” threat declines

POC exploit is publicly available

Discussion on Dark Web

The CVE is assigned a CVSS score

Dark Web activity surfaces again
VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE

Dynamic Nature of Predictive Prioritisation: CVE-2018-17182

- Discussion on Dark Web
- POC exploit is publicly available
- CVE is published on NVD on Sept 19th
- "In the wild" threat declines
- The CVE is assigned a CVSS score
- Dark Web activity surfaces again

Linux Kernel Flaw
Discussion on Dark Web

Dynamic Nature of Predictive Prioritisation: CVE-2018-17182

- POC exploit is publicly available
- "In the wild" threat declines
- The CVE is assigned a CVSS score
- Dark Web activity surfaces again

Linux Kernel Flaw
Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE

Dynamic Nature of Predictive Prioritisation: CVE-2018-17182

- Discussion on Dark Web
- POCl exploit is publicly available
- The CVE is assigned a CVSS score
- Dark Web activity surfaces again

"In the wild" threat declines

CVE is published on NVD on Sept 19th
VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE

Linux Kernel Flaw

Dynamic Nature of Predictive Prioritisation: CVE-2018-17182

- Discussion on Dark Web
- POC exploit is publicly available
- CVE is published on NVD on Sept 19th
- "In the wild" threat declines
- The CVE is assigned a CVSS score
- Dark Web activity surfaces again
Linux Kernel Flaw

VPR INSIGHT - 70 DAYS PRIOR TO CVSS SCORE

The CVE is assigned a CVSS score

Discussion on Dark Web

POC exploit is publicly available

"In the wild" threat declines

Dark Web activity surfaces again

CVE is published on NVD on Sept 19th
# Top Five Vulnerabilities in 2018

<table>
<thead>
<tr>
<th>CVE</th>
<th>CVSSv2 Score (According to NVD)</th>
<th>CVSSv3 Score (According to NVD)</th>
<th>VPR (Vulnerability Priority Rating)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2018-8174</td>
<td>7.6</td>
<td>7.5</td>
<td>9.9</td>
</tr>
<tr>
<td>Windows VB Script</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2018-4878</td>
<td>7.5</td>
<td>9.8</td>
<td>9.5</td>
</tr>
<tr>
<td>Adobe Flash</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2017-11882</td>
<td>9.3</td>
<td>7.8</td>
<td>9.9</td>
</tr>
<tr>
<td>MS Office Memory Corruption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2017-8750</td>
<td>7.6</td>
<td>7.5</td>
<td>9.4</td>
</tr>
<tr>
<td>Internet Explorer Memory Corruption</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CVE-2017-0199</td>
<td>9.3</td>
<td>7.8</td>
<td>9.9</td>
</tr>
<tr>
<td>MS Office/Wordpad Remote Code Execution</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Extracted from the Recorded Future Report “Top Ten Vulnerabilities of 2018” 03/19/19
VPR SCORE CHARACTERISTICS

MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPIO...

Description
The remote Windows host is missing a security update. It is, therefore, affected by the following vulnerabilities:

- Multiple remote code execution vulnerabilities exist in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit these vulnerabilities, via a specially crafted packet, to execute arbitrary code. (CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0148)

- An information disclosure vulnerability exists in Microsoft Server Message Block 1.0 (SMBv1) due to improper handling of certain requests. An unauthenticated, remote attacker can exploit this, via a specially crafted packet, to disclose sensitive information. (CVE-2017-0147)

ETERNALBLUE, ETERNALCHAMPION, ETERNALROMANCE, and ETERNALSYNERGY are four of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. WannaCry / WannaCryp is a ransomware program utilizing the ETERNALBLUE exploit, and EternalRocks is a worm that utilizes seven Equation Group vulnerabilities. Petya is a ransomware program that first utilizes CVE-2017-0146, a vulnerability in Microsoft Office, and then spreads via ETERNALBLUE.

Solution
Microsoft has released a set of patches for Windows Vista, 2008, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10, and 2016. Microsoft has also released emergency patches for Windows operating systems that are no longer supported, including Windows XP 2003, and 8.

See Also
http://www.nessus.org/i/321523e2b
http://www.nessus.org/i/1005561d4d
http://www.nessus.org/i/665169d8f
http://www.nessus.org/i/389d9b5f8b
https://github.com/stamparm/EternalRocks/
http://www.nessus.org/i/5839b5b5b

Output
The remote host is missing one of the following rollup KBs:
- 4012212
- 4013389
C:\Windows\System32\drivers\srv.sys has not been patched.
Remote version: 6.1.7601.17514
Should be: 6.1.7601.23489

Vulnerability Priority Rating (VPR) Key Drivers

Vulnerability Priority Rating: 9.6
CVSS3 Impact Score: 5.9
Threat Recency: 0 to 7 days
Threat Intensity: High
Exploit Code Maturity: High
Age of Vuln: 366 to 730 days
Product Coverage: Low
Threat Sources: Security Research

Risk Information
Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Temporal Vector: E:H/R/L/ODC
CVSS TO VPR: MORE LOW/MEDIUM – FEWER HIGH/CRITICAL

10,214 CVSSv3/v2 High and Critical vulnerabilities become:
• 417 vulnerabilities with a Critical VPR
• 515 vulnerabilities with a High VPR
PRIORITIZING NEAR TERM THREAT

- CVE Count
  - > 5: 24,569
  - > 6: 16,679
  - > 7: 1,118
  - > 8: 388
  - > 9: 178

- CVSS: 65,912
- Predictive Prioritization: 3%

Vulnerability Priority Rating:
- > 5: 24,569
- > 6: 16,679
- > 7: 1,118
- > 8: 388
- > 9: 178

(tenable)
Introducing...Lumin
Leverage machine learning and threat intelligence to prioritize vulnerabilities based on real world risk.

Prioritize assets based on indicators of business value and criticality.

Prioritize based on importance of asset AND risks posed by vulnerabilities on the asset.

**VPR + ACR**

**VULNERABILITY PRIORITY RATING**

**ASSET CRITICALITY RATING**

Focus First On What Matters Most
Risk Exposure Score

- Threat
- Asset
- Vulnerability

Vulnerability Score
Asset Exposure Score
Asset Criticality Score
COMPARE
WITH PEERS AND POPULATION
FOR STRATEGIC DECISION SUPPORT
Recommended workflows

Drill down into specific vulnerabilities and assets for business and technical context to enable more effective remediation.
“By 2022, organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches.”

Thank You
RESOURCES

White Papers

Predictive Prioritization: How to Focus on the Vulnerabilities That Matter Most
https://www.tenable.com/whitepapers/predictive-prioritization-how-to-focus-on-the-vulnerabilities-that-matter-most

Predictive Prioritization: Data Science Lets You Focus on the 3% of Vulnerabilities Likely to Be Exploited
https://www.tenable.com/whitepapers/predictive-prioritization-data-science-lets-you-focus-on-3-percent-of-vulnerabilities

Carnegie Mellon University – “Towards Improving CVSS”

Recorded Future Report “Top Ten Vulnerabilities of 2018” 03/19/19