Navigating the Maze

Making Sense of Vulnerability Risk Indicators

Raffi Erganian, Cofounder – VULNERA
Who We Are

Who We’ve Helped

Raffi Erganian

Joe Luna

[Logos of companies who have been helped]
What we’ll cover

- Vulnerability Context
- NVD Challenges
- The Tools
- Lagging Indicators
- Prioritization
- Easy Wins
Vulnerability Context
NVD Dashboard

CVEs Received and Processed

<table>
<thead>
<tr>
<th>Time Period</th>
<th>New CVEs Received by NVD</th>
<th>New CVEs Analyzed by NVD</th>
<th>Modified CVEs Received by NVD</th>
<th>Modified CVEs Re-analyzed by NVD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Today</td>
<td>85</td>
<td>5</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>This Week</td>
<td>208</td>
<td>15</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>This Month</td>
<td>2229</td>
<td>1305</td>
<td>0</td>
<td>743</td>
</tr>
<tr>
<td>Last Month</td>
<td>2609</td>
<td>2790</td>
<td>0</td>
<td>360</td>
</tr>
<tr>
<td>This Year</td>
<td>4838</td>
<td>4095</td>
<td>0</td>
<td>1103</td>
</tr>
</tbody>
</table>

CVE Status Count

<table>
<thead>
<tr>
<th>Status</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total</td>
<td>239627</td>
</tr>
<tr>
<td>Received</td>
<td>30</td>
</tr>
<tr>
<td>Awaiting Analysis</td>
<td>1268</td>
</tr>
<tr>
<td>Undergoing Analysis</td>
<td>100</td>
</tr>
<tr>
<td>Modified</td>
<td>93109</td>
</tr>
<tr>
<td>Rejected</td>
<td>13968</td>
</tr>
</tbody>
</table>

NVD Contains

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE Vulnerabilities</td>
<td>239627</td>
</tr>
<tr>
<td>Checklists</td>
<td>673</td>
</tr>
<tr>
<td>US-CERT Alerts</td>
<td>249</td>
</tr>
<tr>
<td>US-CERT Vuln Notes</td>
<td>4486</td>
</tr>
<tr>
<td>OVAL Queries</td>
<td>10286</td>
</tr>
<tr>
<td>CPE Names</td>
<td>125970</td>
</tr>
</tbody>
</table>

CVSS V3 Score Distribution

<table>
<thead>
<tr>
<th>Severity</th>
<th>Number of Vulns</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRITICAL</td>
<td>23004</td>
</tr>
<tr>
<td>HIGH</td>
<td>60882</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>59819</td>
</tr>
<tr>
<td>LOW</td>
<td>2526</td>
</tr>
</tbody>
</table>

CVSS V2 Score Distribution

<table>
<thead>
<tr>
<th>Severity</th>
<th>Number of Vulns</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIGH</td>
<td>56837</td>
</tr>
<tr>
<td>MEDIUM</td>
<td>104170</td>
</tr>
<tr>
<td>LOW</td>
<td>19074</td>
</tr>
</tbody>
</table>
Awareness Overload

Existing CVE’s
New CVE’s
Vendor Advisories
Zero-Days
Ransomware Activity
APT Activity

Your Organization

RELEVANT INFORMATION
Tools at our disposal

Industry, community, and vendor risk ratings/metrics

NVD, CVE, CVSS, CWE

CISA KEV, EPSS

Vendor Ratings
NIST & The NVD
The industry standard repository for vulnerabilities

CVSS

CWE

Delay

Accuracy
LAGGING INDICATORS

Exposure Window and Risk Tolerance

- Delayed Response
- Missed Opportunities for Mitigation
- False Sense of Security
- Compliance Risks

19 days  44 days  23 days
CISA KEV  EPSS  Scanners

February 28, 2024
Live Demo
Stop reducing vulnerability risk to a single score.
Prioritizing
Reducing the noise

Know Your Assets

NVD, CVSS, & CWE

CISA KEV / News / VIP-TIP

EPSS?
Know Your Assets
Vulnerability Prioritization

Awareness with Insight drives Action

**Awareness**
News, Peers, Advisories, NVD, CISA KEV, etc

**Insight**
Deployed solutions & technologies

**Action**
Policies, Procedures & Playbooks

**Catalyst**
Awareness vs Technology Based Signals
Awareness

Awareness requires legwork.
You need to keep a pulse on what's happening.
Insight

What tools can you rely on for insight?

- Asset Inventory
- Software Inventory
- Vulnerability Scanners
- SBOM
Challenges

**Insight** is useless without **Awareness**

**Awareness** inactionable without **Insight**

No action without **Insight + Awareness**
Insight Pitfalls

Schedule
Would you run AV once a week?

Port Coverage
False negatives, skipping ports

Agents
False negatives, unsupported assets

Excluded Checks
Missing valuable insight
Easy Wins

CNAs & Vendor Advisories

CVSS & CWE

Leverage TIP/VIP
Easy Wins

Asset & Software Inventory

Edge Device/App List

Vulnerability Scanning

SBOM
Easy Wins

Policies, Procedures, Playbooks

Tabletop – Core Edge Device

Tabletop – 3rd Party Lib

Tabletop – Software
Prioritizing

CVSS, CWE, Advisories, News, Social Media

CISA KEV / VIP-TIP

Vulnerability Scanner Signature & Score

EPSS Score / Percentile
Context is King

Is the vulnerability being actively exploited?

Is it used in ransomware or by APT groups?

Does it have publicly available POC’s?

Does it result in RCE? Code Injection? Authentication bypass?
Get in Touch

Stay up to date with the latest research
Subscribe to our Vulnerability Intelligence Newsletter
raffi@vulnera.com

Follow us on LinkedIn