VRDA
Vulnerability Response Decision Assistance

Hal Burch       Art Manion       Yurie Ito
CERT/CC         CERT/CC         JPCERT/CC

FIRST 2007
VRDA Rationale and Design
Problems

Duplication of effort

• Over 8,000 vulnerability reports in 2007
• Various sources, formats, languages, contents, levels of detail, accuracy, comprehensibility
• Collection and analysis requires significant effort

<table>
<thead>
<tr>
<th>Year</th>
<th>2000</th>
<th>2001</th>
<th>2002</th>
<th>2003</th>
<th>2004</th>
<th>2005</th>
<th>2006</th>
<th>1Q, 2007</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td>1,090</td>
<td>2,437</td>
<td>4,129</td>
<td>3,784</td>
<td>3,780</td>
<td>5,990</td>
<td>8,064</td>
<td>2,176</td>
</tr>
</tbody>
</table>

Total vulnerabilities reported (1995-Q1, 2007): 32,956
Problems (2)

Inconsistent response decisions

- Analysts may disagree
- Analysts apply personal prejudices
- Decisions may not represent organizational values
Problems (3)

Existing metrics insufficient

• Most metrics output global severity values
  – “One size does not fit all.”

• Common Vulnerability Scoring System (CVSS)
  – Contains environmental metrics
  – Focus on base score

• Values vary by organization
  – May respond differently to the same vulnerability
  – Use different software
  – Use the same software in different ways
  – Value information assets differently
Solution

VRDA proposes to answer the question:

*How do I best respond to a given vulnerability report?*

Goals

- Record vulnerability data in structured format
- Support individualized response decision
- Transition organizational knowledge from human analysts to VRDA
- Improve response accuracy and consistency
- Reduce duplication of effort
Audience

System administrators
  - Operational responsibility for fixing systems

CSIRTs
  - Provided advice to system administrators, users

Vendors
  - Product security response teams

Anybody regularly responding to vulnerability reports
Operational Concept
Components

Decisions to make: Tasks
Vulnerability representation: Facts
Product usage: LAPTs
Encoding decision-making: Decision Model
Tasks

Decisions an organization must make
Specific to each VRDA user

Example tasks

• Publish an advisory
• Initiate patch process
• Implement workaround
• Ignore (don’t expend effort on low priority vulnerabilities)
Facts

Properties of vulnerabilities and their environment

Assertions based on available information

- Vulnerability Facts – inherent technical attributes
- World Facts – about environment
- Constituency Facts – specific to VRDA user organization

Balance accuracy, completeness, granularity, cost
LAPTs

Lightweight Affected Product Tags

Problem: Constituency facts cannot be given to you

LAPTs identify products affected by vulnerability

Facilitates lookup of constituency facts

- External feed provides LAPTs for each vulnerability
- Cross-reference with your database
Decision Model

Represents individualized decision-making behavior
Expert system encoding organizational values
Decision trees
Decision Model (2)

Why decision trees?

• Observable, understandable
• Can be created and refined by hand

Model creation

• Design initial model from experience
• Create empirical model based on recorded data
VRDA Usage with KENGINE
KENGINE

VRDA implementation developed by JPCERT/CC
  • Intend to open-source
KENGINE provides consistent analysis and reasoning action
Other KENGINE functions
  • Task management
  • LAPT management
  • Decision tree management
  • Reporting
Minimum resources to handle the maximum number of vulnerabilities
Deployment

Interview user organization

• Determine all possible tasks
  – Identify task dependencies
  – Mandatory/conditional actions do not involve choice, not tasks

• Determine facts
  – Select only facts necessary to make decisions about tasks

Develop decision model

• Teach/train the system using sample VRDA data and choosing appropriate tasks

• Create or modify decision trees manually
KENGINE Customization

Interview session with analysts and system administrators to elicit tasks and facts

What’s the population of this product?

Security products?

Any incident activity?

What kind of service does this system provide? Importance of the system?
Develop Decision Model

Identify dependencies between tasks and facts
KENGINE can generate decision tree automatically

Parameter: What’s the **Population** of this products in my organization?

Value: population **high**. Also this is an **authentication system** for critical service...

Remediation/action:
- Publish alert
- Validate patch immediately
Usage

Get or create VRDA data
Score organization-specific facts
Process vulnerability reports
  • Use the decision model
  • Record actual decisions
Feedback

Compare recommendations with actual decisions
Refine decision making process
  • Update decision model
  • Facts may be missing or inaccurate
  • Tasks may be missing
KENGINE Usage Patterns

Feed service provider

Internet

Intranet

CSIRT users

Light users

Developers, heavy users

View as web page

KENGINE Data format might also available in other XML based format
KENGINE

User ID: test
Password: 

Login

Copyright 2006-2007 JPCERT/CC All Rights Reserved.
## Vulnerability Reports

<table>
<thead>
<tr>
<th>Report ID</th>
<th>Title</th>
<th>Priority [8]</th>
<th>Status</th>
<th>Assign</th>
<th>Task</th>
<th>Created</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>JVN#00000023</td>
<td>MS Updates for Multiple Vuls</td>
<td>1</td>
<td>Pending Close (D2)</td>
<td>admin</td>
<td>Analyze: Yes</td>
<td>'07/08/14</td>
<td>'07/08/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>admin</td>
<td></td>
<td>Security Alert: Notify: Final</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Sharing: Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000029</td>
<td>MS Updates for Multiple Vuls</td>
<td>1</td>
<td>Proposal Req'd (Detailed)</td>
<td>admin</td>
<td>Yes</td>
<td>'07/08/14</td>
<td>'07/08/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>admin</td>
<td></td>
<td>Computed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Notify: No</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Computed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000013</td>
<td>Sourcefire Snort DCE/RPC Preproce...</td>
<td>1</td>
<td>Pending Close (D2)</td>
<td>admin</td>
<td>Yes</td>
<td>'07/06/14</td>
<td>'07/08/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>admin</td>
<td></td>
<td>Refer: Final</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000028</td>
<td>MS SQL Vulnerability</td>
<td>1</td>
<td>Proposal Req'd (Surface)</td>
<td>admin</td>
<td>Yes</td>
<td>'07/08/14</td>
<td>'07/08/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>admin</td>
<td></td>
<td>Alert: No Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Computed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000021</td>
<td>Adobe Acrobat reader</td>
<td>1</td>
<td>Decision Req'd (Surface)</td>
<td>None</td>
<td>Yes</td>
<td>'07/07/14</td>
<td>'07/08/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>None</td>
<td></td>
<td>Refer: No Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Computed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000025</td>
<td>GNUPG Vulnerability</td>
<td>1</td>
<td>Detailed Analysis Req'd</td>
<td>admin</td>
<td>Yes</td>
<td>'07/08/14</td>
<td>'07/08/14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>admin</td>
<td></td>
<td>Notify: No Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Computed</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Vulnerability Report Detail

** General Information ** Edit

- Report ID: JVN#00000023
- Title: MS Updates for Multiple Vuls
- Memo:
- Status: Pending Close (D2)
- Created By: admin
- Tri Handler: admin  Vul Handler: admin

- Surface Completed: 2007/08/14 23:12
- Detailed Completed: 2007/08/14 23:28
- Decision Finalized: 2007/08/14 23:29
- Report Closed:

** Analysis Information **

- LAPT - Edit
Selected LAPTS
[Microsoft-Excel][Microsoft-InternetExplorer][Microsoft-Windows-Vista][Microsoft-Windows-XP][Microsoft-Word]

- FACT - Edit
Impact:
The impact of the vulnerability is:
- None  Low  Medium  High  Unknown

Access_Required:
The type of network and/or physical access required to exploit this vulnerability is:
- Routed  Non-routed  Local  Physical  Unknown

Authentication_Required:
What level of authentication does exploiting this vulnerability require?
- None  Limited  Standard  Privileged  Unknown
## LAPT Management

<table>
<thead>
<tr>
<th>Name</th>
<th>Related Reports</th>
<th>FACT Organization Used</th>
<th>Importance</th>
<th>Last Checked</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe-Acrobat</td>
<td>0</td>
<td>Yes</td>
<td>Low</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Adobe-Acrobat-Reader</td>
<td>1</td>
<td>Yes</td>
<td>Medium</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Apache</td>
<td>1</td>
<td>Yes</td>
<td>High</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Apple-MacOS-X</td>
<td>2</td>
<td>Yes</td>
<td>Low</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Apple-QuickTime</td>
<td>2</td>
<td>No</td>
<td>None</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Apple-Safari</td>
<td>1</td>
<td>Yes</td>
<td>Low</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Bind</td>
<td>1</td>
<td>Yes</td>
<td>High</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Cisco-IOS-10</td>
<td>1</td>
<td>Yes</td>
<td>High</td>
<td>61days</td>
<td>Edit</td>
</tr>
<tr>
<td>Debian</td>
<td>1</td>
<td>No</td>
<td>None</td>
<td>61days</td>
<td>Edit</td>
</tr>
</tbody>
</table>
## Task Workflow

<table>
<thead>
<tr>
<th>Report ID</th>
<th>Task</th>
<th>Decision</th>
<th>Priority</th>
<th>Task Status</th>
<th>Update</th>
<th>Memo</th>
<th>Details</th>
<th>Last Updated</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>JVN#00000005</td>
<td>Analyze</td>
<td>Yes</td>
<td>1</td>
<td>Not Started</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000003</td>
<td>Analyze</td>
<td>Yes</td>
<td>1</td>
<td>In Progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000010</td>
<td>Analyze</td>
<td>Yes</td>
<td>1</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000023</td>
<td>Analyze</td>
<td>Yes</td>
<td>1</td>
<td>Not Started</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000020</td>
<td>Analyze</td>
<td>Yes</td>
<td>1</td>
<td>In Progress</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000002</td>
<td>Analyze</td>
<td>Yes</td>
<td>1</td>
<td>Completed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JVN#00000012</td>
<td>Analyze</td>
<td>Yes</td>
<td>1</td>
<td>Not Started</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Decision Tree

Name: Security_Alert

Master : Star

Tree Tag Name : MASTER-Generated

Comment : 

- Consider field "Importance"
  - Unknown -> Consider field "Impact"
  - Unknown -> Consider field "Required_Actions"
  - Unknown -> Consider field "Authentication_Required"
    - Unknown -> "No_Act"
    - Privileged -> "No_Act"
    - Standard -> "No_Act"
    - Limited -> "Refer"
    - None -> "Notify"
  - Complex -> "No_Act"
  - Simple -> "Notify"
  - High -> "Alert"
  - Medium -> "Notify"
  - Low -> "Refer"
  - None -> "No_Act"
- High -> Consider field "Impact"
  - Unknown -> Consider field "Activity"
    - Unknown -> "No_Act"
    - Our Incident -> "Alert"
Task Deviation Report

Task: Analyze  Review Decision

<table>
<thead>
<tr>
<th></th>
<th>'06/07</th>
<th>'06/08</th>
<th>'06/09</th>
<th>'06/10</th>
<th>'06/11</th>
<th>'06/12</th>
<th>'07/01</th>
<th>'07/02</th>
<th>'07/03</th>
<th>'07/04</th>
<th>'07/05</th>
<th>'07/06</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed Dec. &lt;=&gt; Final Dec.</td>
<td>0%</td>
<td>9%</td>
<td>0%</td>
<td>25%</td>
<td>55%</td>
<td>48%</td>
<td>0%</td>
<td>51%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>44%</td>
</tr>
<tr>
<td>Final Dec. &lt;=&gt; Task Comp.</td>
<td>0%</td>
<td>18%</td>
<td>0%</td>
<td>10%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>2%</td>
</tr>
</tbody>
</table>
Progress Report

Handling Volume of Vul. Reports

- Not Assigned: 10% (2)
- Proposal Req’d (Surface): 5% (1)
- Decision Req’d (Surface): 13% (2)
- Detailed Analysis Req’d: 5% (1)
- Proposal Req’d (Detailed): 14% (3)
- Pending Close (D2): 48% (10)
Handling Volume Report

Handling Volume of Vul. Reports

- No.1: Vuls Created
- No.2: Surface Analysis
- No.3: Detailed Analysis
- No.4: Decisions Made
- No.5: Tasks Completed
- No.8: Vuls Closed

07/01, 07/02, 07/03, 07/04, 07/05, 07/06, 07/07, 07/08
Future

KENGINE availability

- JPCERT/CC intends to provide open-source
- Documented in Japanese and English

JPCERT/CC

- VRDA data feeds with vulnerability and world facts
- Pilot program in progress
- Deployment consulting

CERT/CC

- Developing pilot program