TCVM: A New Approach to Targeting Risk with Context-Aware Vulnerability Management

David Anteliz | Senior Sales Engineer | Central
David.Anteliz@SkyboxSecurity.com
Who We Are

Silicon Valley HQ
Offices around the globe

Attack Surface Management
Visibility & Analytics to maintain resilience

Fastest-growing company in our space
$270M funding since February 2016

700+ active customers
50 countries, all verticals
Current Industry Challenges
Most Breaches are Preventable

97% of breaches are avoidable through standard controls*

- No visibility of the environment
- Lack of actionable intelligence
- Disjointed security tools and data
- Lack of cross-functional expertise

Organizations don’t understand their attack surface

*According to Verizon Data Breach Investigation Report
#1 Overwhelming Number of Vulnerabilities

- 700 – 1,100 new vulnerabilities every month
- Historically systems have been poorly patched
- Scanner generates a LOT of data
- People end up focusing on the “criticals”
#2 It’s not just about the criticals

Most Exploited Vulnerabilities were Not Ranked “critical”
#3 Not just a Zero Day problem

85% of exploited vulnerabilities were more than 2 years old

- Verizon Data Breach Investigations Report
Traditional Approach Causes Pain – Broken Process

**Discovery**
- Infrequency of scans
- Disruptive scans
- Unable to scan all assets
- Multiple environments
- Lack of authenticated scanning

**Risk Analysis**
- Too much data
- No context of existing controls
- Hard to correlate data from multiple sources
- Threat landscape is dynamic
- Hard to prioritize by business impact
- Exploitability is not considered
- Likelihood of exploitability is not considered
- Lack of prioritisation by SLA/Risk

**Remediation**
- Hard to convert vulnerability info to patch needs
- Difficult to find alternative remediation options
- Unnecessary patching
- Critical risks open for too long
- Poor SLA management
- Poor communication
- Poor tracking of remediation
Understanding the IT/OT Asset Relationships

Level 5: Corporate Network
Level 4: Bus Apps
Level 3.5: Data DMZ
Level 3: Control System LAN
Levels 0-2: Basic Control, Supervisory, Process
Skybox: Ingredients for Effective Vulnerability Prioritization

**Vulnerability-Centric**
Criticality of vulnerability (CVSS score, exploitation impact, public exploit available)

**Context-Centric**
Business criticality, value and exposure of an asset (internet-facing, third-party access, contains sensitive data, provides business-critical functions)

**Threat-Centric**
Actively being targeted by malware, ransomware, exploit kits and threat actors in the wild
How is Skybox helping?
Skybox Security Suite

Improve Customer’s Existing Resources
Asset Management

Vulnerability and Threat Management
Research Lab

Vulnerability Scanners

Firewalls

IPS

Security Policy Management

Vulnerability Control

Network Assurance

Change Manager

DeepSight/iDefense
(Leading Edge)

SIEM/IT-GRC
(Trailing Edge)

Ticketing Systems
(Remedy/ServiceNow)
Improve Customer’s Existing Resources

Integrates with 120+ technologies
Skybox Vulnerability Database & Attack Vector Intelligence

- Skybox Research Lab aggregates 20+ vulnerability and threat feeds
- More than 50,000 vulnerabilities on 1,800 products
- Including products, vulnerabilities, IPS signatures, patches, malware patterns
- CVE compliant, CVSS v3 standard
- Proprietary intelligence added by analysts
  - Exploitation pre-conditions
  - Likelihood of attack
  - Conflict resolution
- Updated daily

<table>
<thead>
<tr>
<th>ADVISORIES</th>
<th>SCANNERS</th>
<th>IPS</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adobe</td>
<td>eEye Retina</td>
<td>Fortinet FortiGate</td>
<td>CERT</td>
</tr>
<tr>
<td>Cisco PSIRT</td>
<td>IBM Scanner</td>
<td>HP TippingPoint</td>
<td>IBM X-Force</td>
</tr>
<tr>
<td>Microsoft Security Bulletin</td>
<td>McAfee Foundstone</td>
<td>IBM Proventia</td>
<td>Mitre CVE</td>
</tr>
<tr>
<td>Oracle</td>
<td>Qualys Guard</td>
<td>McAfee IPS</td>
<td>NIST’s NVD</td>
</tr>
<tr>
<td>RedHat</td>
<td>Rapid7</td>
<td>Palo Alto Networks</td>
<td>OSBDV</td>
</tr>
<tr>
<td></td>
<td>Nexpose</td>
<td>Cisco Sourcefire</td>
<td>Rapid7 Metasploit</td>
</tr>
<tr>
<td></td>
<td>Tenable Nessus</td>
<td></td>
<td>Secunia</td>
</tr>
<tr>
<td></td>
<td>Tripwire IP360</td>
<td></td>
<td>Symantec</td>
</tr>
</tbody>
</table>

- Vulnerabilities with no CVE
- Remediation solutions
- Cross-references

Updated daily skyboxsecurity.com
How this works at a high level
## Inherable Control

### Vulnerability Occurrences Analysis: Exposed (Direct & Indirect)

<table>
<thead>
<tr>
<th>Risk</th>
<th>Exposure</th>
<th>Title</th>
<th>Source</th>
<th>ID</th>
<th>CVE</th>
<th>Asset</th>
<th>OS</th>
<th>Service Ports</th>
<th>BIND (domain:0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote</td>
<td>Skybox</td>
<td>SBV-51699</td>
<td>CVE-2015-14</td>
<td>dmi_dmi0 [192.168.33.33]</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (domain:0)</td>
<td></td>
</tr>
</tbody>
</table>

### Vulnerability Occurrence: ISC Bind 10.x Remote Shell Injection Vulnerability in Patch(1)

**General**

- Malware & Exploits
- CVSS
- Asset
- Service
- Tickets
- Risk Profile
- Solutions

**Title:** ISC Bind 10.x Remote Shell Injection Vulnerability in Patch(1)

**ID:** SBV-51699

**CVE:** CVE-2015-14
## Vulnerability Control

### Organization (Overall - Vul Level)
- Acme Inc.
- Asia-Pac Operations (Medium)
- Europe Operations (Critical)
- US Headquarters (Critical)
- Exposure by Threat
- Analyses
  - Public Analyses
  - Risks - Advanced
  - Vulnerabilities
    - By Exposure and Exploitability
      - All Vulnerabilities
      - Inaccessible
      - Exposed (Direct & Indirect)

### Directly Exposed
- Indirectly Exposed
- Exploitable Vulnerabilities
- Exposed and Exploitable
- Critical Vulnerabilities
- Excluded
- Unknown Exposure
- Vulnerability Dictionary
- Cisco IOS Vuls
- Ransomware Vulnerabilities
- By Operating System
- New Vulnerability Occurrences
- Dictionary
- Vulnerability Dictionary
- New Vulnerability Definitions
- Worm Dictionary
- Vulnerability Count Analyses

## Vulnerability Occurrences Analysis: Directly Exposed

### Risk
- Direct

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Title</th>
<th>Source</th>
<th>ID</th>
<th>CVE</th>
<th>Asset</th>
<th>OS</th>
<th>Service Ports</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-51699 CVE-2016-14</td>
<td>dmz_dms1</td>
<td>192.170</td>
<td>Linux</td>
<td>53/TCP</td>
<td>BIND (dom)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_2</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_2</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_2</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_2</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_2</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_4</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_5</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>ISC Bind 10.x Remote Shell Injection Vuln... Skybox SBV-47012 CVE-2014-41</td>
<td>dmz_web_server_6</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>IBM WebSphere 5.3 HTTP Server for 2055</td>
<td>0.0</td>
<td>0.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_1</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_4</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_8</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct</td>
<td>Microsoft IIS 6.0 and 7.5 Remote DoS Vuln... Skybox SBV-35467</td>
<td>dmz_web_server_9</td>
<td>Windows</td>
<td>80/TCP</td>
<td>IS (http)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Vulnerability Occurrence: ISC Bind 10.x Remote Shell Injection Vulnerability in Patch(1)

#### General
- Malware & Exploits
- CVSS
- Asset
- Service
- Tickets
- Risk Profile
- Solutions

**Title:** ISC Bind 10.x Remote Shell Injection Vulnerability in Patch(1)

**ID:** SBV-51699

**CVE:**
### Vulnerability Control

#### Prioritization Center

- Vulnerability Control
  - Organization (Overall - Vul Level) - Acme Inc.
  - Asia-Pac Operations (Medium)
  - Europe Operations (Critical)
  - US Headquarters (Critical)
- Exposure by Threat
  - Sources
    - External
    - Internal
    - Both
- Vulnerabilities
  - Exposure
    - Direct
    - Indirect
  - Impact
    - Accessible
    - Exploitable
- Directly Exposed
  - Exploitable Vulnerabilities
  - Exposed and Exploitable
  - Critical Vulnerabilities
  - Excluded
  - Unknown Exposure
  - Vulnerability Dictionary
  - Cisco IOS Vuls
  - Ransomware Vuls
- By Operating System
  - New Vulnerability Occurrences
  - Dictionary
  - Vulnerability Dictionary
  - New Vulnerability Definitions
- Worm Dictionary
- By Scan Type
- Threats and Attacks
- Private Analyses

### Vulnerability Occurrences Analysis: Indirectly Exposed

<table>
<thead>
<tr>
<th>Exposure</th>
<th>Title</th>
<th>Source</th>
<th>ID</th>
<th>CVE</th>
<th>Asset</th>
<th>OS</th>
<th>Service Ports</th>
<th>Service Name</th>
<th>Service Version</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indirect</td>
<td>(cpaur2013-1899555) Oracle Database Server on Windows Remote Code Execution</td>
<td>Skybox</td>
<td>SBV-39126</td>
<td>CVE-2013-1534</td>
<td>finance_db_1</td>
<td>Windows 8</td>
<td>1521/TCP</td>
<td>Oracle (nvl2)</td>
<td>(nvl2)</td>
<td>Found</td>
</tr>
</tbody>
</table>


**General**
- Malware & Exploits
- CVSS
- Asset
- Service
- Tickets
- Risk Profile
- Solutions

**Title:** [cpaur2013-1899555] Oracle Database Server on Windows Remote Code Execution

**ID:** SBV-39126

**CVE:** CVE-2013-1534

**Description:**
Oracle Database Server 11.2.0.2 and 11.2.0.3 on Windows is prone to a remote code execution vulnerability with root privileges. It is exploitable over HTTP.
### Vulnerability Occurrences Analysis: Exploitable Vulnerabilities

<table>
<thead>
<tr>
<th>Risk</th>
<th>Exposure</th>
<th>Title</th>
<th>Source</th>
<th>ID</th>
<th>CVE</th>
<th>Asset</th>
<th>OS</th>
<th>Service Ports</th>
<th>Service Name</th>
</tr>
</thead>
</table>

**1,026 Vulnerability Occurrences**

**Vulnerability Occurrence: Buffer Overflow in NFS mountd Allows Root Access**

**Title:** Buffer Overflow in NFS mountd Allows Root Access

**Description:** Buffer overflow in NFS mountd gives root access to remote attackers. Mostly in Linux/Unix systems.
## Vulnerability Occurrences Analysis: Exposed and Exploitable

<table>
<thead>
<tr>
<th>Risk</th>
<th>Exposure</th>
<th>Title</th>
<th>Source</th>
<th>ID</th>
<th>CVE</th>
<th>Asset</th>
<th>OS</th>
<th>Exploit Availability</th>
<th>Service Ports</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_101</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_111</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_211</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_311</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_411</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_511</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_611</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_711</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_811</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_911</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_111</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_111</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_211</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_311</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_411</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_511</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_611</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_711</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_811</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Indirect</td>
<td>cpunct2012-1515893</td>
<td>Skybox</td>
<td>SBV-36637</td>
<td>CVE-2012-3137 finance_db_911</td>
<td>Windows Se.</td>
<td>Exploit Available</td>
<td>1521/TCP</td>
<td>Oracle (net8)</td>
<td></td>
</tr>
</tbody>
</table>

### 13 Vulnerability Occurrences

#### Vulnerability Occurrence: Apache Chunked-Encoding Memory Corruption Vulnerability

- **General**
  - Malware & Antivirus
  - CVE
  - Aetz
  - Service
  - Tickets
  - Risk Profile
  - Solutions
Skybox – Security Middleware platform
Thank you
Questions?