NTIA Supply Chain Transparency

2018-07-19
Art Manion
amanion@cert.org
@zmanion

About
- Art Manion
  Vulnerability Analysis Technical Manager
  (“/” Principal Engineer)
  CERT Coordination Center (CERT/CC)

Defender use cases
- Are things I use vulnerable?
- Are parts I use to make things vulnerable?
- Are the sectors I’m responsible for affected?

Puzzle pieces
- Standard inventory
- Component relationships
- Vulnerability mapping
Defender use cases

End user
Consumer
System administrator

Vulnerability prioritization
- Are the things I use or depend on vulnerable?
  Which things?
- Even more important during attack

Procurement and maintenance
- Are the things I'm buying or renting vulnerable?
- Indicator of security quality
  - Existence of SBoM
  - List of upstream components
  - Status of known vulnerabilities
- End-of-life for component, and vendor

Last available SBoM
Defender use cases

Vendor
Supplier
Provider

Vulnerability prioritization
- Are the parts that I use to make things vulnerable? Which parts?
- Even more important during attack

Procurement and maintenance
- Indicator of security quality
- Supply chain hygiene
  - Fewer components, fewer break/fix events
Defender use cases

Critical infrastructure protection
Public safety
Policy

Are the sectors I care about vulnerable?

- Do those sectors use vulnerable components?
- How prevalent?
- Is the vulnerability exposed to attack?
Puzzle pieces

Break it down

Standard inventory format
- Appropriate level of abstraction
- SWID? SPDX?
- Probably not CPE

Component relationships
- A includes B

Vulnerability mapping
- B is vulnerable to CVE-2010-0738
- A may be vulnerable to CVE-2010-0738
- Requires vulnerability identification
Vendor Information for VU#228519
Wi-Fi Protected Access (WPA) handshake traffic can be manipulated to induce nonce and session key reuse

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Status</th>
<th>Date Notified</th>
<th>Date Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>9front</td>
<td>Affected</td>
<td>-</td>
<td>19 Oct 2017</td>
</tr>
<tr>
<td>Actiontec</td>
<td>Affected</td>
<td>30 Aug 2017</td>
<td>20 Oct 2017</td>
</tr>
<tr>
<td>ADTRAN</td>
<td>Affected</td>
<td>-</td>
<td>19 Oct 2017</td>
</tr>
<tr>
<td>Aerohive</td>
<td>Affected</td>
<td>30 Aug 2017</td>
<td>17 Oct 2017</td>
</tr>
<tr>
<td>Alcatel-Lucent Enterprise</td>
<td>Affected</td>
<td>28 Aug 2017</td>
<td>08 Nov 2017</td>
</tr>
<tr>
<td>Android Open Source Project</td>
<td>Affected</td>
<td>28 Aug 2017</td>
<td>08 Nov 2017</td>
</tr>
<tr>
<td>Apple</td>
<td>Affected</td>
<td>28 Aug 2017</td>
<td>01 Nov 2017</td>
</tr>
<tr>
<td>Arch Linux</td>
<td>Affected</td>
<td>28 Aug 2017</td>
<td>17 Oct 2017</td>
</tr>
<tr>
<td>Aruba Networks</td>
<td>Affected</td>
<td>28 Aug 2017</td>
<td>09 Oct 2017</td>
</tr>
<tr>
<td>AsusTek Computer Inc.</td>
<td>Affected</td>
<td>28 Aug 2017</td>
<td>19 Oct 2017</td>
</tr>
<tr>
<td>AVM GmbH</td>
<td>Affected</td>
<td>-</td>
<td>24 Oct 2017</td>
</tr>
<tr>
<td>Barracuda Networks</td>
<td>Affected</td>
<td>28 Aug 2017</td>
<td>24 Oct 2017</td>
</tr>
<tr>
<td>Broadcom</td>
<td>Affected</td>
<td>30 Aug 2017</td>
<td>17 Oct 2017</td>
</tr>
</tbody>
</table>

Here's a list

Created with significant manual effort
Component relationships
CVE-2010-0738 JBoss JMX-Console access control vulnerability

- Patched in April 2010

Exploited by SamSam in 2016

- Ransomware
- Health care providers
- Schools

Did vendors know they used JBoss?

Did users know they used JBoss?

https://threatpost.com/3-2-million-servers-vulnerable-to-jboss-attack/117465/

Follett Destiny Library Manager
Destiny uses JBoss, JBoss vulnerable to CVE-2010-0738, ∴ Destiny vulnerable to CVE-2010-0738
https://blog.talosintelligence.com/2016/04/jboss-backdoor.html

Erie County Medical Center
Hancock Health
Hollywood Presbyterian Medical Center? (2010 JBoss JMX-Console or ~2015 Java deserialization?)