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

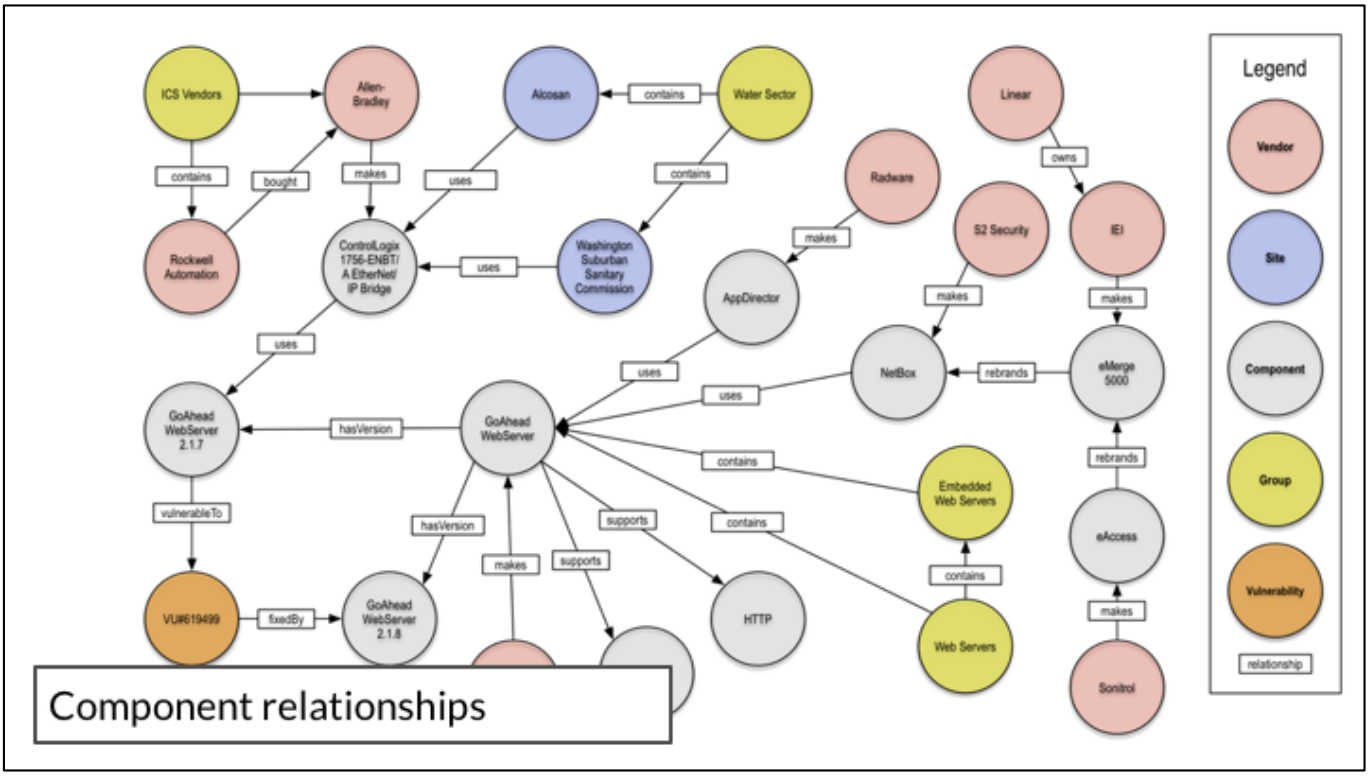
Here's a list

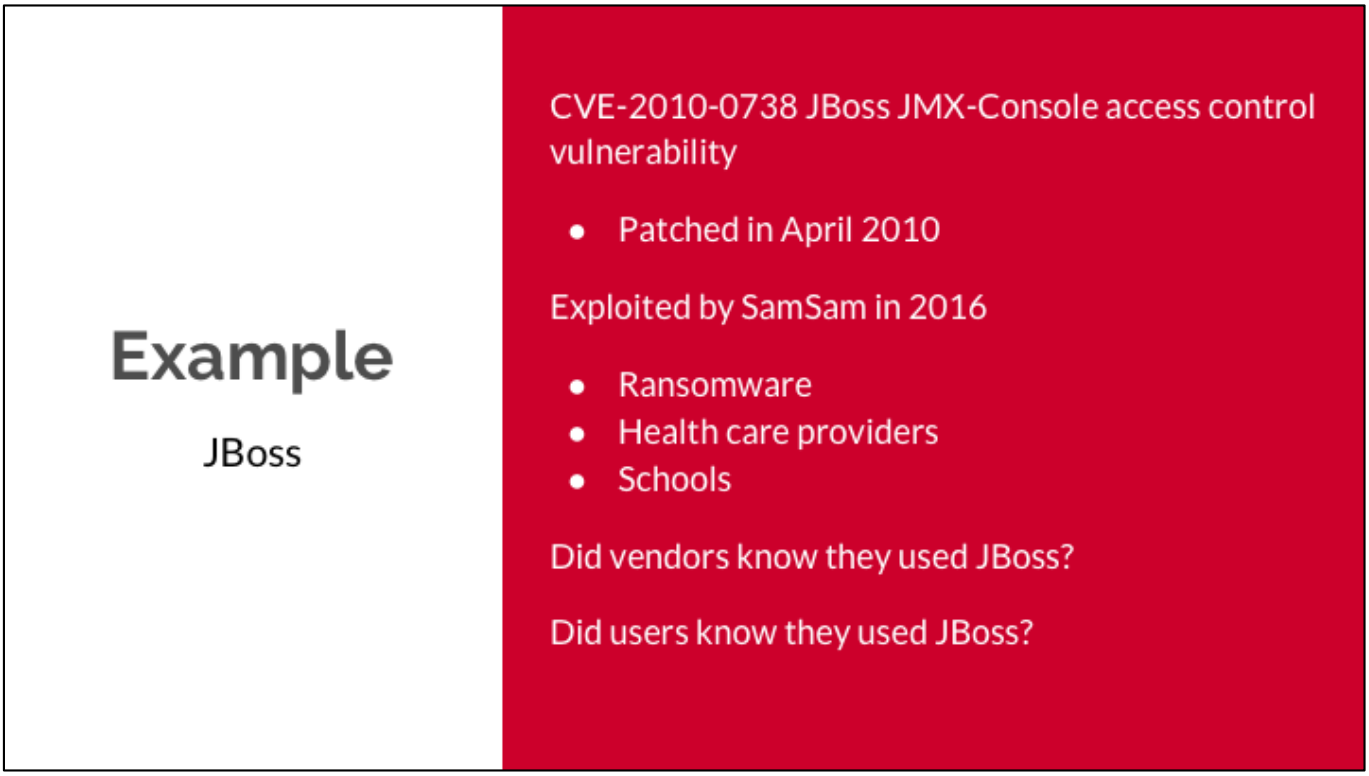
Created with significant manual effort

Vendor Information for VU#228519

Wi-Fi Protected Access (WPA) handshake traffic can be manipulated to induce nonce and session key reuse

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


ICS Vendors
Allen-Bradley
Alcosan
contains
Water Sector
Linear
contains
bought
makes
uses
contains
owns
Radware
Rockwell Automation
ControlLogix 1756-ENBT/A EtherNet/IP Bridge
uses
Washington Suburban Sanitary Commission
makes
S2 Security
IEI
AppDirector
makes
makes
uses
NetBox
rebrands
eMerge 5000
GoAhead WebServer 2.1.7
hasVersion
GoAhead WebServer
uses
uses
contains
Embedded Web Servers
rebrands
vulnerableTo
hasVersion
supports
contains
eAccess
makes
supports
contains
VU#619499
fixedBy
GoAhead WebServer 2.1.8
HTTP
Web Servers
makes
Sonitrol
Component relationships
Legend
Vendor
Site
Component
Group
Vulnerability
relationship



https://blog.varonis.com/new-samsam-ransomware-still-exploits-old-jboss-vulnerability/
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?)
https://slate.com/technology/2018/06/how-hospitals-can-protect-themselves-against-ransomware.html
https://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/