Secure Application Deployment in the Age of Continuous Delivery

OPENSOURCE: Open Standards
#whoami – Tim Mackey

- Current roles: Senior Technical Evangelist; Occasional coder
  - Previously XenServer Community Manager
- Cool things I’ve done
  - Designed laser communication systems
  - Early designer of retail self-checkout machines
  - Embedded special relativity algorithms into industrial control system
- Find me
  - Twitter: @TimInTech
  - SlideShare: slideshare.net/TimMackey
  - LinkedIn: www.linkedin.com/in/mackeytim
Security reality

You can only protect what you know about.
Defense in depth matters.
Attacks are big business

In 2015, 89% of data breaches had a financial or espionage motive

Source: Verizon 2016 Data Breach Report
Police Pay Off Ransomware Operators, Again

Law enforcement agencies are proving to be easy marks -- but are they any worse than the rest of us?

Police departments are proving to be easy marks for ransomware operators -- but perhaps no more so than anyone else. Recently, reports are stacking up of police departments paying attackers ransoms -- payments in the $300 to $500, made in Bitcoins -- for the recovery of encrypted files and equipment.
Open source ubiquity makes it ready target

GitHub

EASY ACCESS TO SOURCE CODE

nuget

VULNERABILITIES ARE PUBLICIZED

NIST

OPEN SOURCE ISN’T MORE OR LESS SECURE THAN CLOSED SOURCE – ITS JUST EASIER TO ACCESS

EXPLOITS ARE PUBLISHED

YouTube
Anatomy of a new attack

Potential Attack ➔ Test against platforms ➔ Deploy

Iterate

Don’t forget PR department
Open source enters through many channels...

...and vulnerabilities can come with it.
Who is responsible for code and security?


Chad innocentkiller at gmail.com
Mon Dec 21 20:37:34 UTC 2015

- Messages sorted by: [date] [thread] [subject] [author]

We would like to announce the release of MediaWiki 1.26.2, 1.25.5, 1.24.6, and 1.23.13.

These are maintenance releases to fix regressions introduced in the previous release.

Download links are given at the end of this email.

== Maintenance fixes ==
(7121892) Verbose special pages resulted in fatal errors.

== Note about 1.24.0 changes ==
Please note that 1.24.6 marks the end of support for the 1.24.x series of releases. Technically this ended a few weeks ago with the release of 1.26.0.

However, 1.24.5 had issues (along with other versions), so it was thought fair to fix them.
Increasing number of OSS vulnerabilities

Open Source Vulnerabilities Reported Per Year

Reference: Black Duck Software Knowledgebase, NVD
Automated tools miss most open source vulnerabilities

Static & Dynamic Analysis
Only discover common vulnerabilities

Undiscovered vulnerabilities are too complex and nuanced

3,000+ disclosed in 2014
Less than 1% found by automated tools
What do these all have in common?

<table>
<thead>
<tr>
<th>Component</th>
<th>Heartbleed</th>
<th>Shellshock</th>
<th>Freak</th>
<th>Ghost</th>
<th>Venom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovered by</td>
<td>Riku, Antti, Matti, Mehta</td>
<td>Chazelas</td>
<td>Beurdouche</td>
<td>Qualys researchers</td>
<td>Geffner</td>
</tr>
</tbody>
</table>

Component:
- OpenSSL
- Bash
- OpenSSL
- GNU C library
- QEMU

Discovered by:
- Riku, Antti, Matti, Mehta
- Chazelas
- Beurdouche
- Qualys researchers
- Geffner
Understand application contents

- 67% of applications reviewed contained open source security vulnerabilities
- 40% of open source vulnerabilities in each application were rated "severe"
- 105 average number of open source components in each application
- 100% on average the companies were using 100% more open source than they originally believed
- 22.5 average number of open source component vulnerabilities in each application
- 1,894 days average age of open source component vulnerabilities at scan time
- 10% of the applications included the Heartbleed vulnerability

Source: 2016 Open Source Security Report
84% of all cyber attacks happen on the application layer

SOURCE: SAP

EXPANDING SECURITY RISKS

1998

2008

2016

Network  Web  SaaS  Mobile  Cloud  IoT
Misaligned security investment

Application Security Faces Most Threats

But Network Security Attracts the Highest Investment

SOURCE: PONEMON INSTITUTE STATE OF APPLICATION SECURITY RISK MANAGEMENT REPORT
Distinct areas of risk

- Open source license compliance
  - Ensure project dependencies are understood
- Use of vulnerable open source components
  - Is component a fork or dependency?
  - How is component linked?
- Operational risk
  - Can you differentiate between “stable” and “dead”?
  - Is there a significant change set in your future?
  - API versioning
  - Security response process for project
Total Quality Management Philosophies

- Detect problems before product ships
- Select components based on trust
- Continuously identify issues and improve
- Empower employees to solve problems
- Implement the Deming Cycle
  - Plan for change and analyze risk
  - Do execute the plan in small steps
  - Check the results against the plan
  - Act on results to improve future outcomes
- Manage with facts
Software development lifecycle

Idea → Spec → Design → Code → Test → Release
Software development lifecycle – threat model

- As part of the specification and design, threat models are often created.
Software development lifecycle – static analysis

- As part of the specification and design, threat models are often created.
- During code creation and commits, static analysis is performed.
Software development lifecycle – dynamic analysis

- As part of the specification and design, threat models are often created.
- During code creation and commits, static analysis is performed.
- Testing usually includes some form of dynamic testing.
Traditional operations release process

- Release
- Update Spec
- Assess
- Deploy
- Measure
- Monitor
- Scale
Oops – a vulnerability is disclosed – now what?

- **DEVELOP**
  - Bug Tracking
  - Remediate and track license compliance and security vulnerabilities

- **SCM**
  - FULL APP SEC VISIBILITY INTEGRATION

- **BUILD**
  - SCAN APPLICATIONS WITH EACH BUILD VIA CI INTEGRATION

- **PACKAGE**
  - BUILD / CI SERVER

- **DEPLOY**
  - DELIVERY PIPELINE

- **PRODUCTION**
  - CONTINUOUS MONITORING OF VULNERABILITIES
  - SCAN APPLICATIONS AND CONTAINERS BEFORE DELIVERY
Integrations matter ...
Containers for application management

- 73% of enterprises are currently using containers for development & testing* 
- 92% of organizations are using or considering Docker containers* 
- 53% of IT operations & development decision-makers say security is their biggest concern about containers** 
- 30% of containers distributed in official Docker repositories have high priority security vulnerabilities***

*According to a survey by ClusterHQ
**According to a Forrester study sponsored by Red Hat
***According to BanyonOps
Knowledge is key. Can you keep up?

Robert 2015-07-13 23:41:12 UTC

description:

When the thisansszip pointer variable on line 1257 is updated, thisansszip = anssizp2, i.e. assigned a new address, this change causes the thisansszip pointer variable used in the recvfrom function on line 1282 to use the wrong size if a new buffer is created after the thisansszip address has been changed at line 1257.

The size of the buffer used will be what was stored at the address assigned at line 1257, and not the size of the newly created buffer.

The program will crash if the calculated size of the buffer used is 0. The recvfrom function will not crash, but any further accesses to the buffer where the bytes read was 0 from the recvfrom function will crash the program.

Vuln: CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow
Knowledge is key. Can you keep up?

- **Vuln Introduced**: May 2008
- **Bug Reported**: glibc
- **CVE Assigned**: CVE-2015-7547

Florian Weimer 2016-02-16 14:11:42 UTC

This was assigned CVE-2015-7547. This bug was introduced in glibc 2.9. For details, please see:

https://sourceware.org/ml/libc-alpha/2016-02/msg00416.html

Vuln: CVE-2015-7547: glibc getaddrinfo stack-based buffer overflow

Low Security Risk
Knowledge is key. Can you keep up?

National Cyber Awareness System

Vulnerability Summary for CVE-2015-7547

Original release date: 02/18/2016
Last revised: 06/23/2016
Source: US-CERT/NIST

Overview

Multiple stack-based buffer overflows in the (1) send dg and (2) send vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.

Impact

CVSS Severity (version 3.0):
CVSS v3 Base Score: 8.1 High

Moderate Security Risk
Low Security Risk

Vuln: CVE-2015-7547

glibc

Introduced May 2008

Vuln Reported July 2015

CVE-2015-7547

National Vulnerability Database Vuln Published Feb 18 - 2016
Knowledge is key. Can you keep up?

2/22 Update
VMware Knowledge Base article 2144032 continues to be updated when new workarounds, patches, and updated releases for CVE-2015-7547 become available. In addition, we have released VMware Security Advisory VMSA-2016-0002 to alert customers to the release of a patch that addresses CVE-2015-7547 on ESXi 5.5.

2/23 Update
VMware Security Advisory VMSA-2016-0002 has been updated after the release of a patch that addresses CVE-2015-7547 on ESXi 6.0. We’ve also updated VMware Knowledge Base article 2144032 and added more workarounds, patches, and updated releases for CVE-2015-7547.

3/29 Update
Today new versions of vCenter Server Appliance (VCSA), 5.0 U3f, 5.1 U3c, and 5.5 U3c, which address CVE-2015-7547 have been released. Earlier in February we released workarounds for VCSA. As mentioned before, update releases that address this CVE on VMware appliances, along with workarounds and patches, are found in VMware Knowledge Base article 2144032. This KB will continue to be updated on a regular basis.
Who Handles Known Vulnerabilities

1/2 of respondents said that no one has responsibility for identifying & tracking remediation.

Development organizations are 33% more likely to have responsibility for identifying and tracking vulnerability remediation than security organizations.

Source: Future of Open Source 2016 Survey
A complete solution …

**SELECT**
- Choose Open Source
  - Proactively choose secure, supported open source

**VERIFY**
- Inventory Open Source
  - Identify vulnerabilities during development
- Map Existing Vulnerabilities

**REMEDiate**
- Fix Vulnerabilities
  - Tell developers how to remediate

**MONITOR**
- Track New Vulnerabilities
  - Alert newly disclosed vulnerabilities in production

Maintain accurate list of open source components throughout the SDL
Black Duck Created an Industry

- **1800+ CUSTOMERS**
- 6 of the top 8 mobile handset vendors
- 6 of the top 10 banks
- 7 of the top 10 SOFTWARE COMPANIES (44% OF TOP 100)

**USE BLACK DUCK SOFTWARE**

**FORTUNE 100**

- **27**
- **24 COUNTRIES**

**AWARD FOR INNOVATION**
- SBANE

**GARTNER GROUP “COOL VENDOR”**

**RANKED #38 OUT OF 500 SECURITY COMPANIES**

**INNOVATIVE TECHNOLOGY OF THE YEAR - SECURITY**

**SOFTWARE 500 COMPANIES**

**7 YEARS IN A ROW**

**OVER TWO HUNDRED THIRTY EMPLOYEES**

**7 YEARS IN A ROW FOR SECURITY INNOVATION**
Comprehensive KnowledgeBase

• Largest database of open source project information in the world.

• Vulnerabilities coverage extended through partnership with Risk Based Security.

• The KnowledgeBase is essential for identifying and solving open source issues.
We need your help

Knowledge is power
- Know what’s running and why
- Define proactive vulnerability response process
- Don’t let technology hype cycle dictate security

Invest in defense in depth models
- Don’t rely on perimeter security to do heavy lifting
- Do look at hypervisor & container trends in security
- Make developers and ops teams part of the solution
- Do embed security into deployment process

Together we can build a more secure data center
Free tools to help

- Docker Container Security Scanner
  - [https://info.blackducksoftware.com/Security-Scan.html](https://info.blackducksoftware.com/Security-Scan.html)

- 14 Day Free Trial to Black Duck Hub
  - [https://info.blackducksoftware.com/Demo.html](https://info.blackducksoftware.com/Demo.html)

- Red Hat Atomic Host Integration (Requires Black Duck Hub)
  - `atomic scan --scanner blackduck [container]`