EMORY UNIVERSITY

EMORY HEALTHCARE

Office of Information Technology

IT Briefing

February 21, 2013

Goizueta Foundation Center

W100

IT Briefing Agenda

- IT Security Update — Derek Spransy
- Kronos Timekeeping — Michael Davidson
- Major Incidents Update — Missie Martin/Anne Marie Alexander/ Kevin Chen
- IT Briefing Update — Wade Moricle

Derek Spransy

Sr Information Security Specialist, Information Security

IT Security Update

February's Big Numbers

6,806,249

3,759

3

February's Big Numbers

6,806,249

Number of malicious URLs blocked

3,759

Number of malware downloads blocked

3

Number of end user complaints

Malicious Content Filtering

Malware Download Blocked

Effective December 21, 2012

If you are seeing this message, it is because you have visited or you have been redirected to a site that is known to contain malicious content, or attempted to download a file which appears to contain malicious code. For more information, please visit the Malicious Content Filtering page. If you feel that you've reached this page in error or have any questions, you may contact the Emory University Service Desk by calling 404-727-7777.

File name: [redacted].exe

Web Page Blocked

Effective December 21, 2012

If you are seeing this message, it is because you have visited or you have been redirected to a site that is known to contain malicious content, or attempted to download a file which appears to contain malicious code. For more information, please visit the Malicious Content Filtering page. If you feel that you've reached this page in error or have any questions, you may contact the Emory University Service Desk by calling 404-727-7777.

URL: www.[redacted]

Category: malware-sites

Security Awareness

February:

- Malicious Content Filtering

IT Security Update

Java Security

- Java continues to be a primary vector for exploitation
- The biggest problem is an inability to patch
- Working to identify widely-used Java applications at Emory that require older JRE releases
- Kronos has been identified as one of these applications

Michael Davidson

Manager, PeopleSoft/Kronos Middleware,
Enterprise Applications

Kronos Timekeeping: Client Java Versions

Java Client for Kronos

Kronos is a web-based application that leverages a Java Runtime Environment (JRE) on the client for Kronos-delivered applets.

Kronos certifies their software to specific versions of Java, based on the version of Kronos being run.

Java Client for Kronos (cont.)

In the IT industry, Java updates are required to mitigate security threats / exposures.

Historically, Kronos only certified their application to ONE Java update.

Kronos 6.3 was certified to *Java 6 update 29.*

Java Client for Kronos (cont.)

Enterprise Applications and Information Security teams have been meeting with Kronos executives and engineers to address the timeliness of Kronos Java update certifications.

The Emory team pursued answers from Kronos regarding their Java strategies:

- short-term
- long-term

Java Client for Kronos (cont.)

SHORT-TERM STRATEGY

Kronos is now certifying their application dot release versions to certain Java update versions.

However…

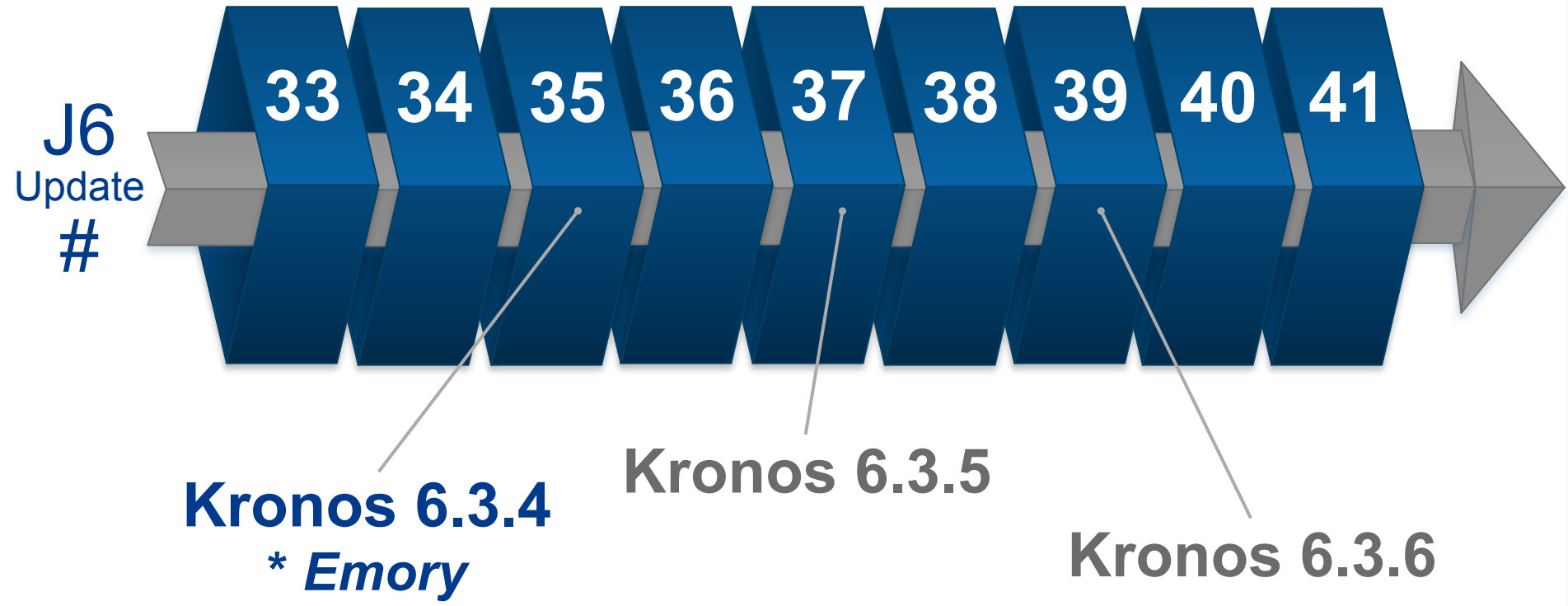
Kronos is only certifying back **TWO** dot releases.

Current = Kronos 6.3.6

Emory = Kronos 6.3.4

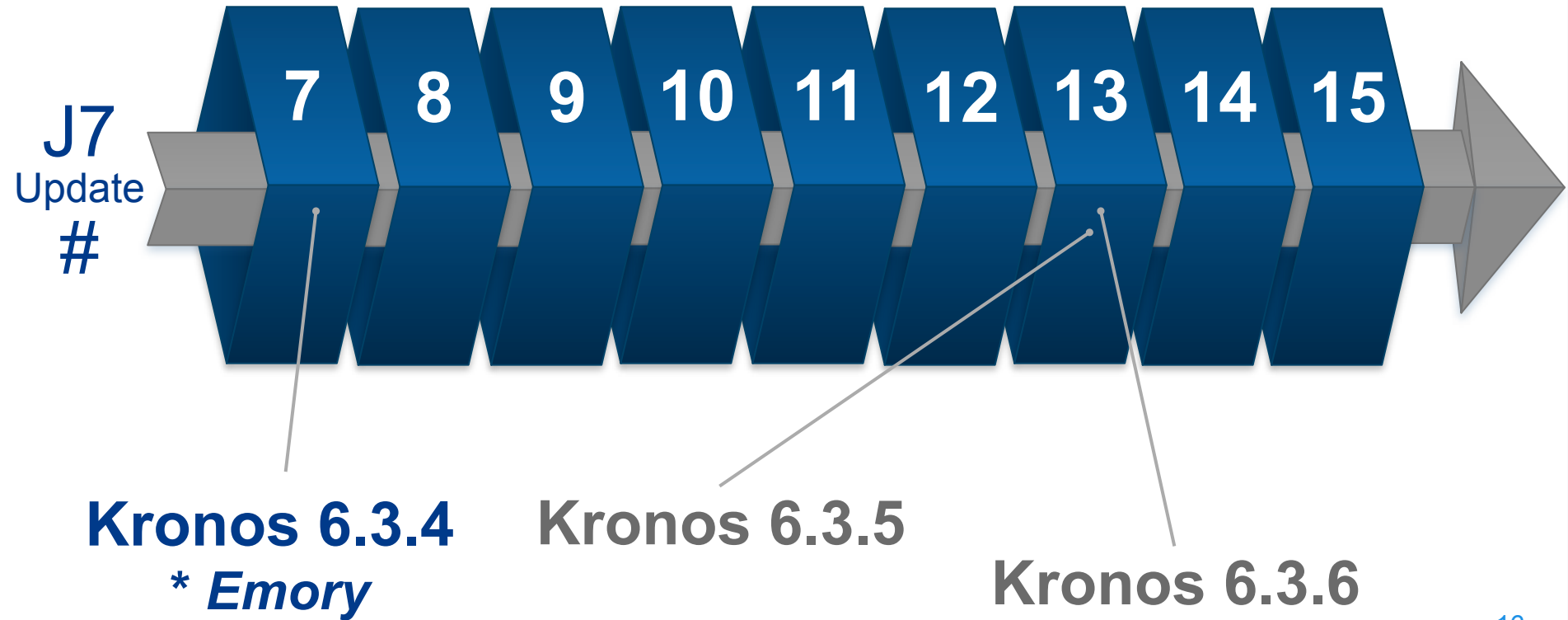
Supported Java Versions for Kronos

Oracle Java 6



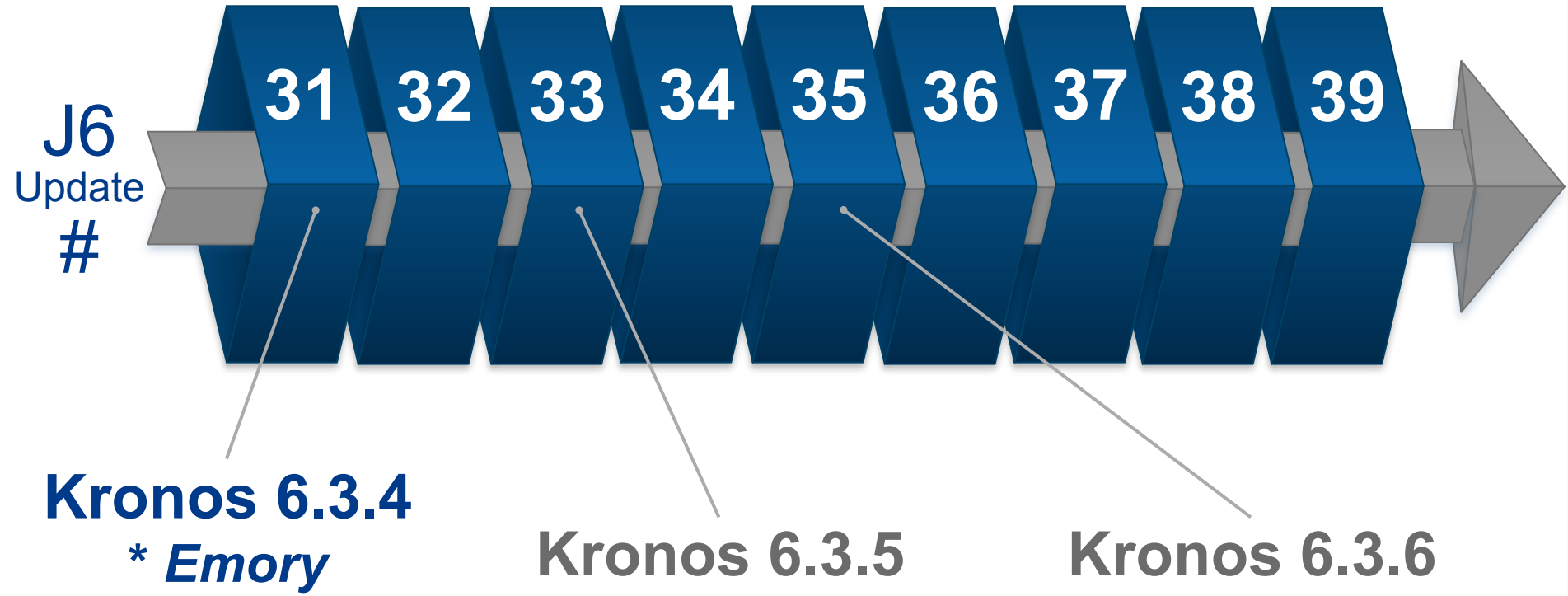
Supported Java Versions for Kronos

Oracle Java 7



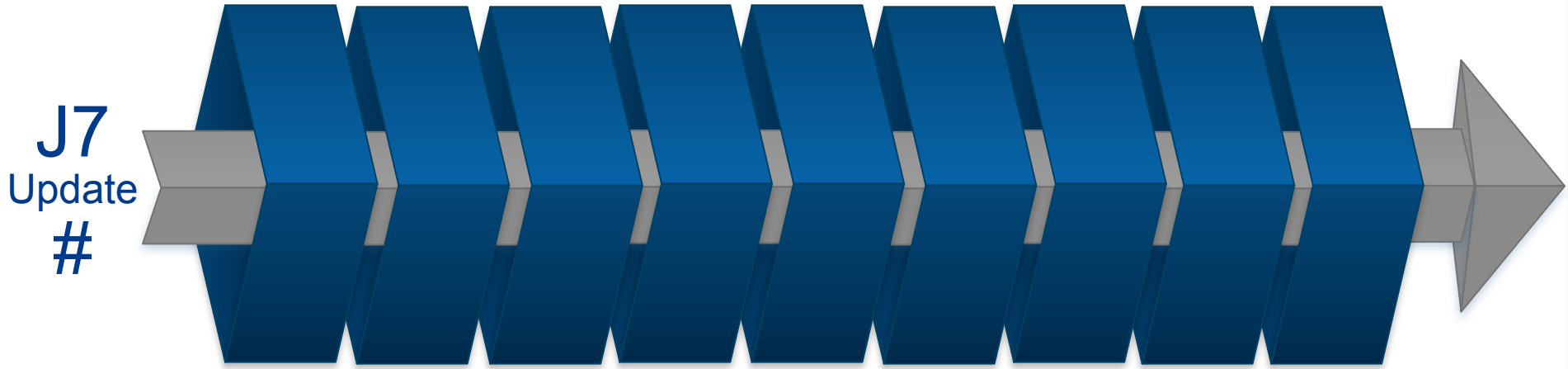
Supported Java Versions for Kronos

Apple Java 6



Supported Java Versions for Kronos

Apple Java 7



Not Supported

Java Client for Kronos

MEDIUM-RANGE PLAN

To increase security for Java applets, Kronos will start digitally signing their applets this year.

Target release: Kronos 6.3.8 (late June, 2013)

Java Client for Kronos

LONG-TERM ARCHITECTURE

The Kronos executive team has shared with Emory about their long-term strategic direction.

Kronos plans to not use Java applets in the future.

Java Client for Kronos

LONG-TERM ARCHITECTURE

HTML5 and CSS3

Target release date?

Unknown

Questions?

Missie Martin
IT Service Manager, ITSMO, Integration
Anne Marie Alexander
Sr. Manager, ID Management, Integration
Kevin Chen
Sr. Manager, Information Technology, Integration

Major Incidents Update (P1 – Critical)

Emory Unplugged (Authentication)

- P1-Critial Incidents since January 1
  - INC01764851 (01/28/13)
  - INC01768190 (02/01/13)
  - INC01769204 (02/04/13)
- Root Cause
  - Increased authentication traffic from wireless overloaded the existing capacity
- Service Improvement Plan
  - Implemented hardware load balancing
  - Added 2 additional RADIUS Servers
  - Adding Microsoft NPS Proxy Servers
  - Researching options to further optimize service

Web Hosting (ColdFusion9)

- P1-Critical Incidents since January 1
  - INC01757536 (01/14/13)
  - INC01757868 (01/15/13)
  - INC01759460 (01/16/13)
  - INC01771519 (02/07/13)

- Root Cause
  - In the current ColdFusion/JBoss environment, there are too many applications deployed to a single JBoss instance

- Service Improvement Plan
  - Migrate all UTS hosted websites to a new ColdFusion9 (CF9) configuration, including sites currently on CF7
    - Gives each site its own JBoss server for CF9 requests
    - User testing began on 02/11
    - Migrations are tentatively scheduled for 2/25 & 2/27

Other P1-Critical Incidents

- INC01771519 (02/01) – www.emory.edu was unavailable for approx. 10 minutes. The Web Hosting servers were rebooted and the service came back on-line. The root cause is still under investigation.

- INC01776202 (02/18) – Oxford Facilities shut down power to repair a sewage leak. This caused a loss of Network services for 1 ½ hours.

- INC01776054 (02/18) – Emory iTunes U was unavailable for 1 hour due to an incorrect database connection string after the upgrade from 10g to 11g.

Major Incidents Update

Wade Moricle

Marketing and Communication Specialist, Integration

IT Briefing Update

Current Status

- Yearly Review
- Distribution
- Location
- Rebroadcast
- Removal of old calendar entries

You can always reach me at:

wade.moricle@emory.edu

What's next?

IT Briefing Update

Thank you for coming!