RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

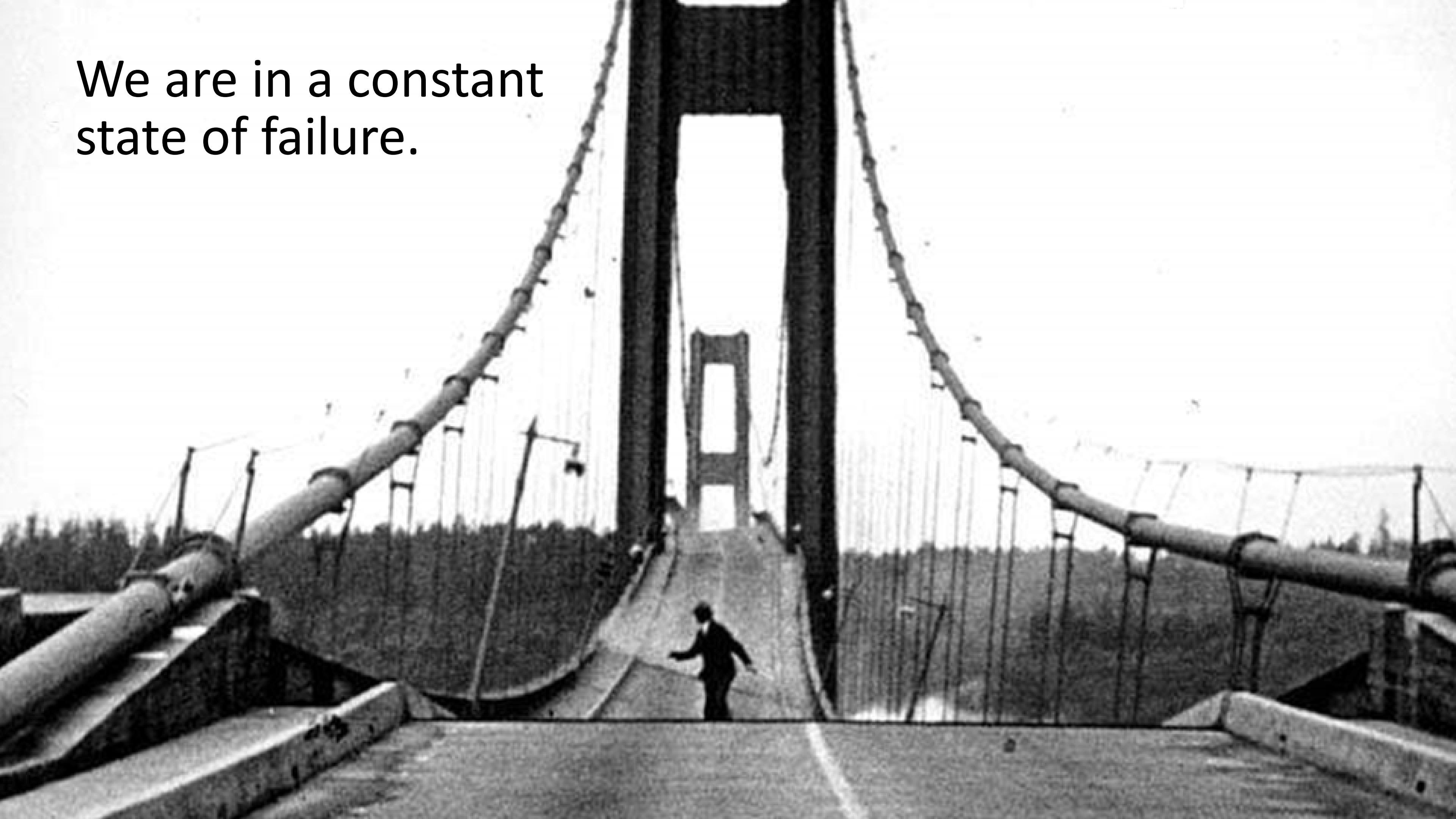
SESSION ID: TECH-W02

EVOLVE OR DIE: HOW TO STOP GETTING SLAUGHTERED DUE TO BAD VULNERABILITY MANAGEMENT

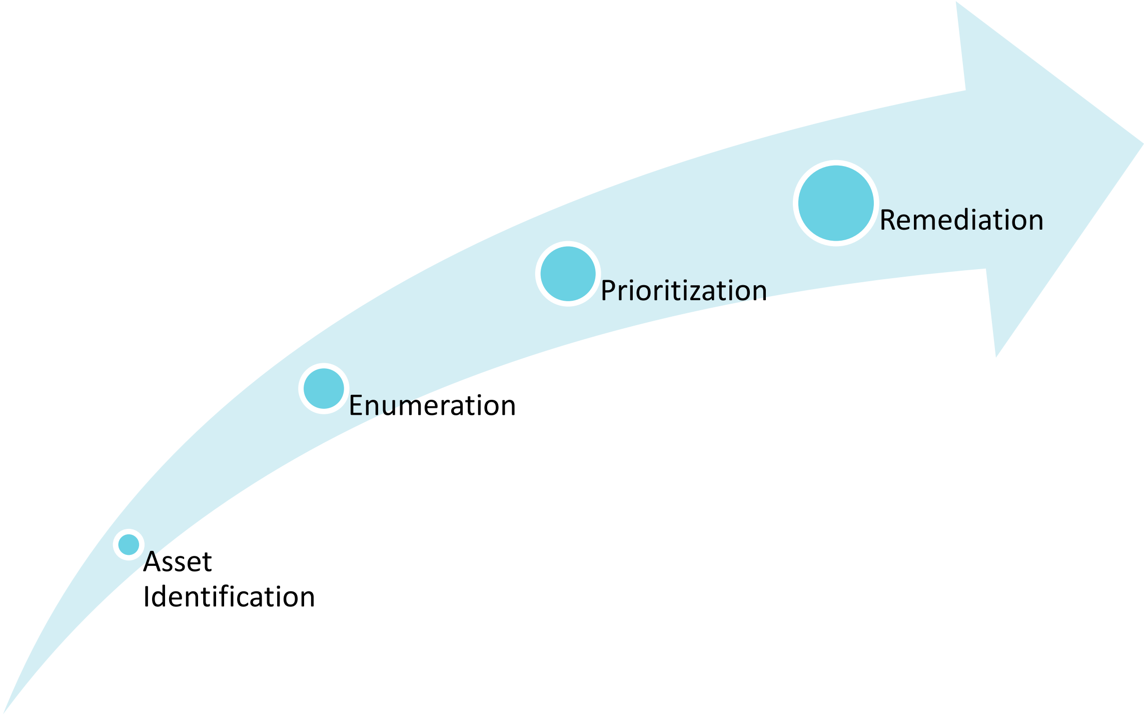
Josh Zelonis

Senior Analyst
Forrester
@jz415

We are in a constant state of failure.



Vulnerability Management Process



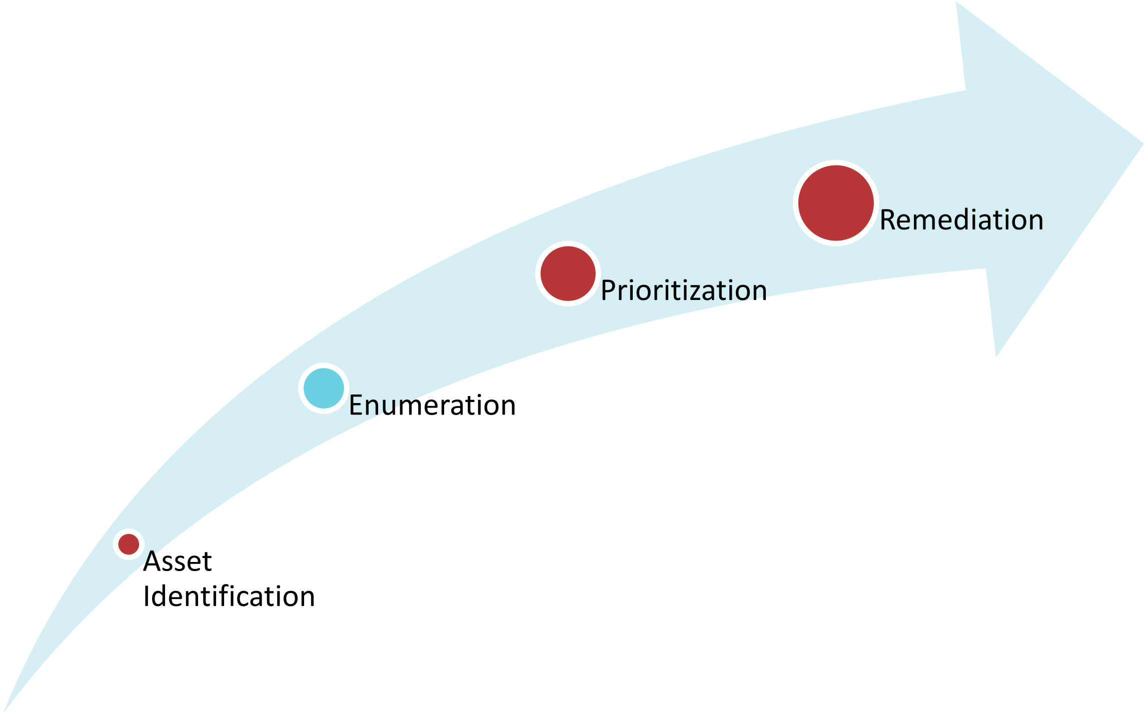
Asset Identification

Enumeration

Prioritization

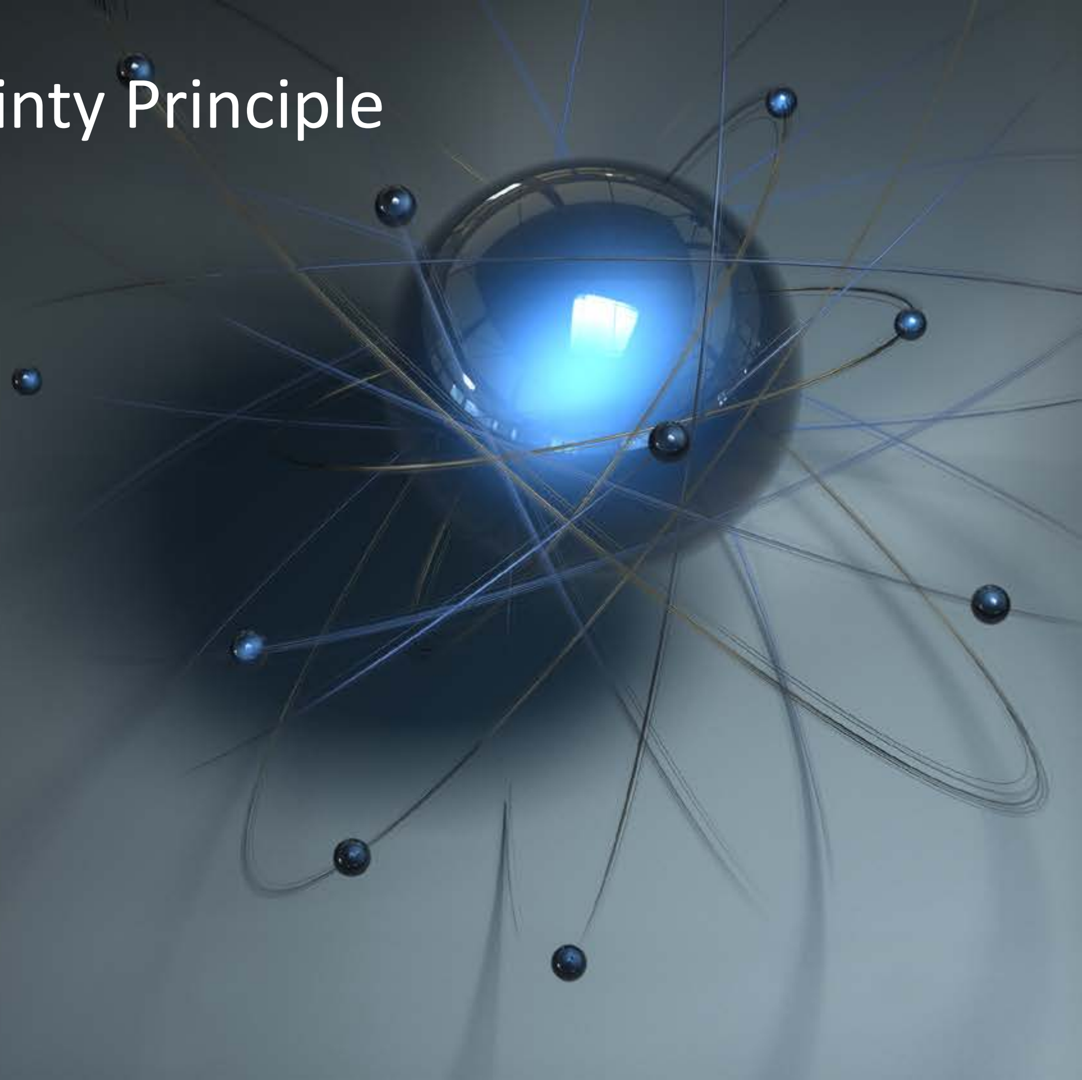
Remediation

Vulnerability Management Process



VULNERABILITY MANAGEMENT IS A MAINTENANCE TASK THAT BEGINS AND ENDS WITH OPERATIONS

The Heisenberg Uncertainty Principle of Asset Management



Take Charge Of Asset Management

- Queryable infrastructure is the fabric of a good CMDB
- Consider the operational benefits of EDR products
  - Remote management software
  - Creates queryable infrastructure
  - Ability to detect misuse
- Use scanners to identify unmanaged hosts
  - Embrace coverage as a critical metric

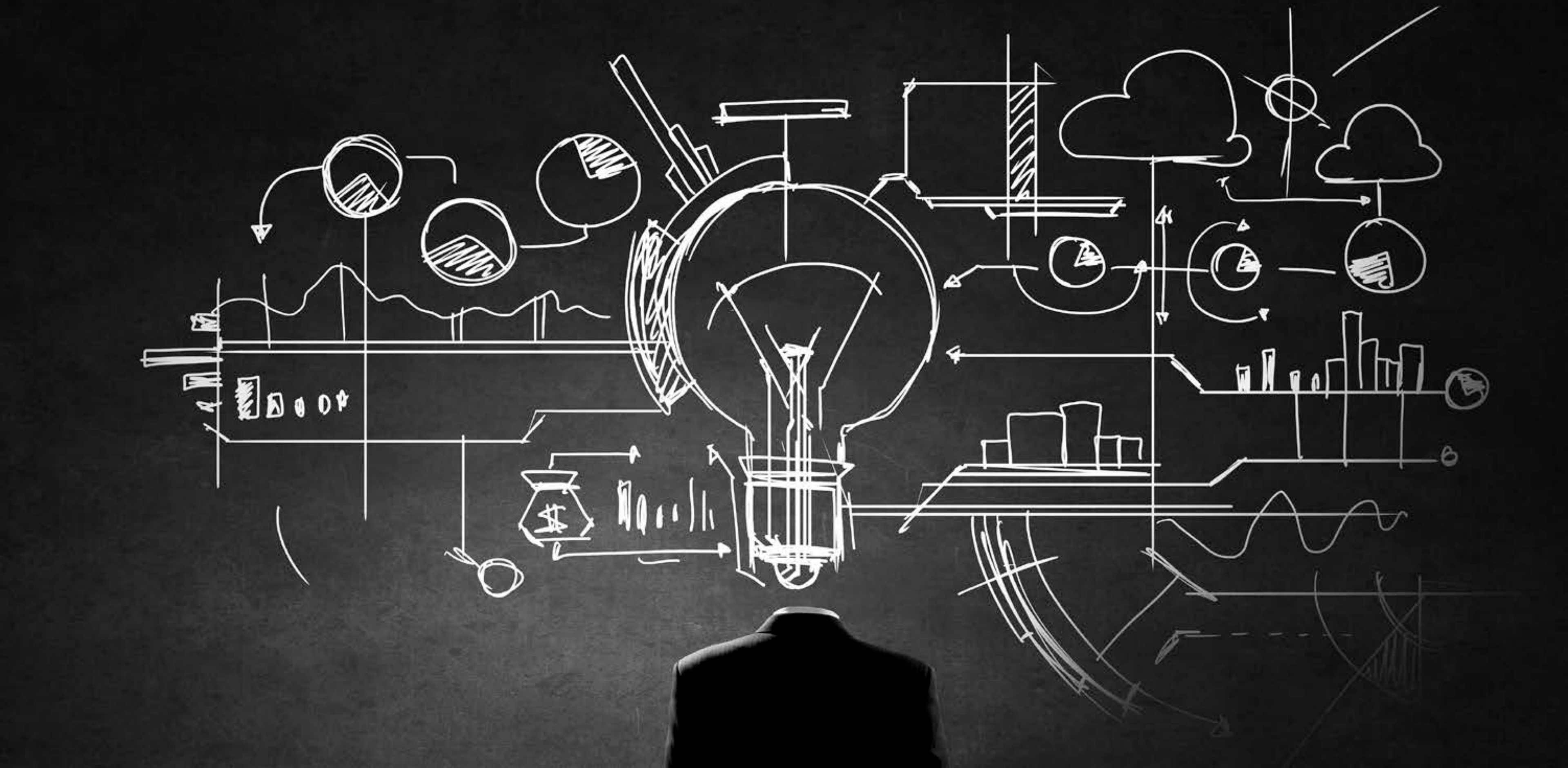
IN 2017, OVER 29% OF CVE HAD A SEVERITY OF HIGH OR CRITICAL.

Define SLA's By Priority, Not Severity

#RSAC

	Vulnerability Severity			
Asset Criticality	**Low**	**Medium**	**High**	**Critical**
High	Priority 3	Priority 2	Priority 1	Priority 1
Medium	Priority 4	Priority 3	Priority 2	Priority 2
Low	Priority 5	Priority 4	Priority 3	Priority 3

It's Time To Start Using Threat Intelligence Strategically



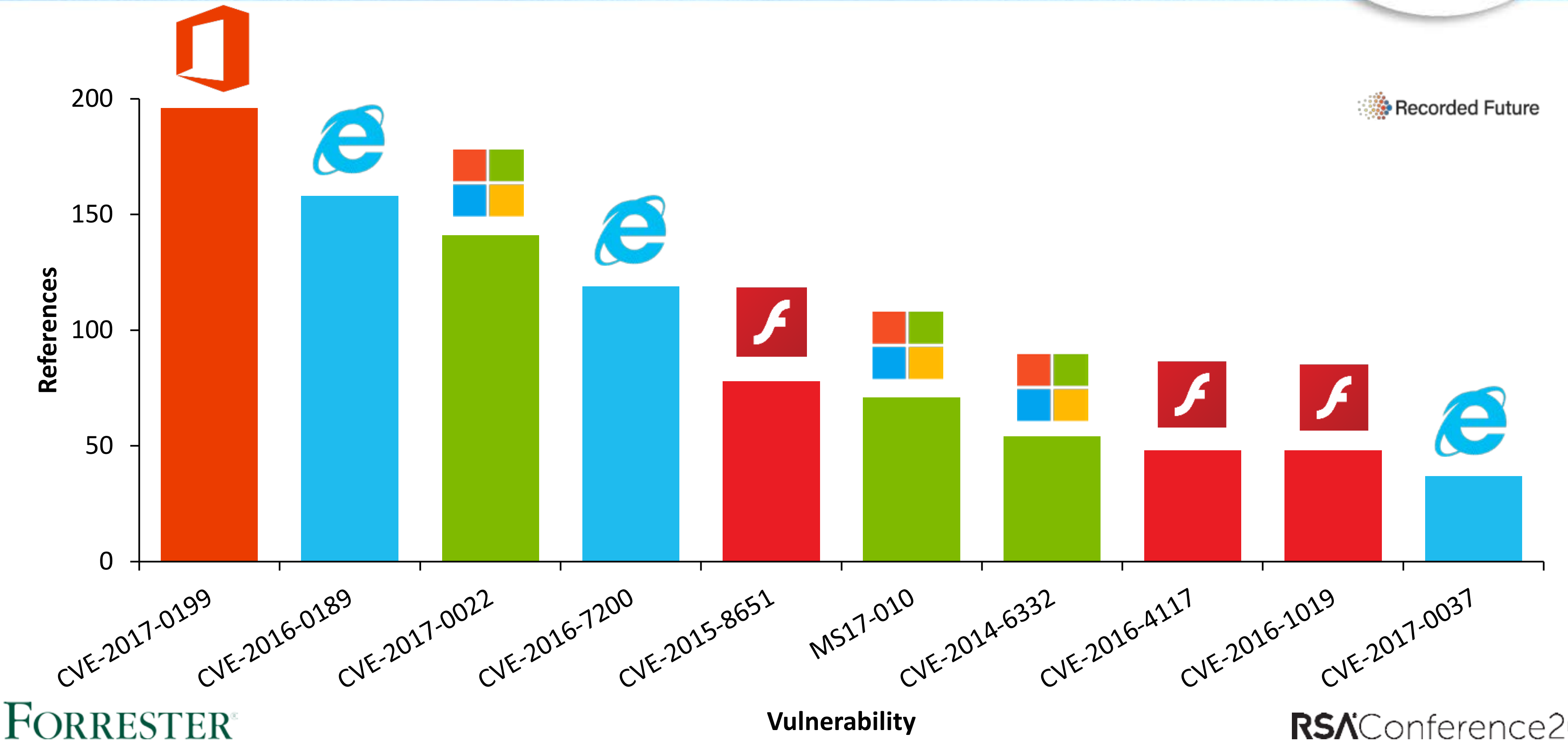
KEY QUESTION: HOW COULD AN ATTACKER EXPLOIT THIS VULNERABILITY?

Dissect Delivery and Exploitation

A Cursory Analysis of Meltdown

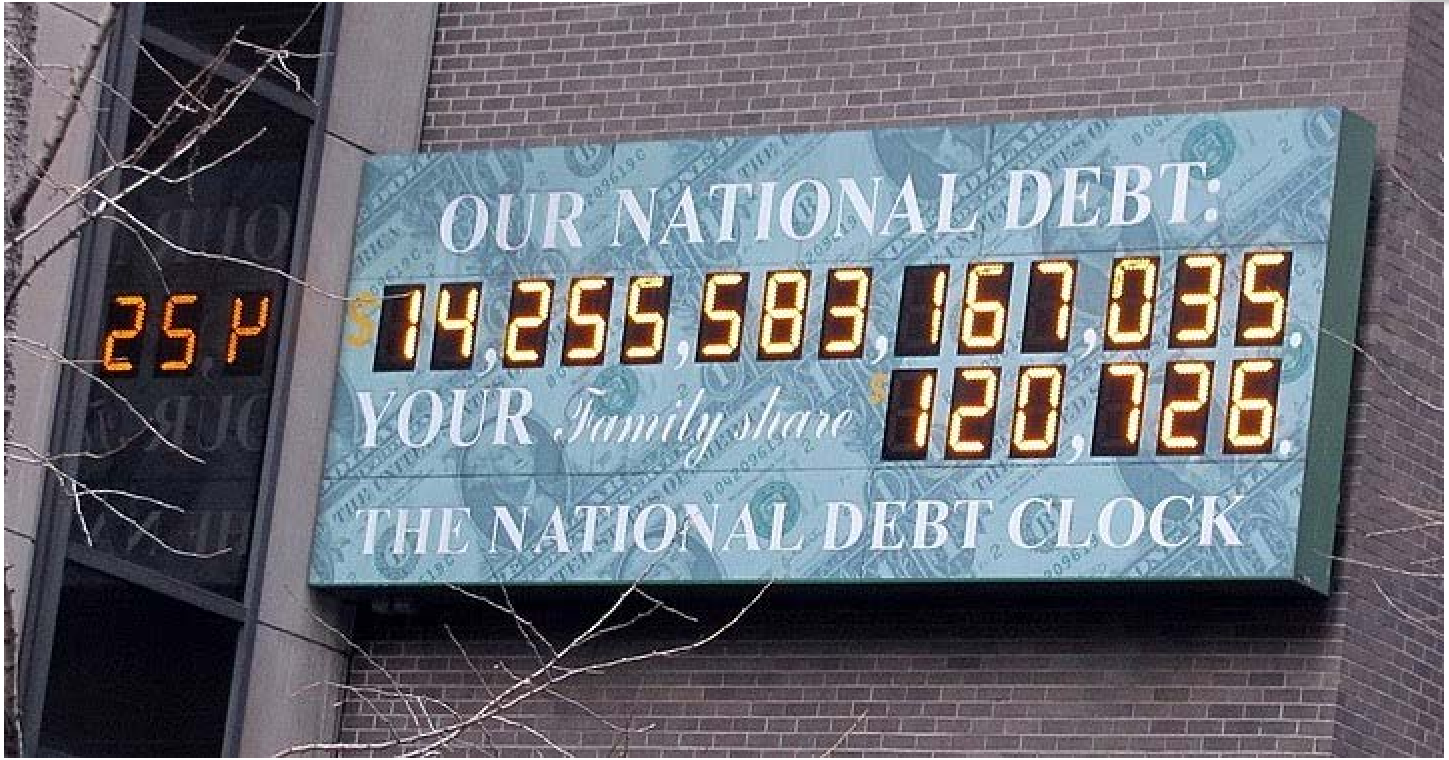
- Can be delivered to browser using JavaScript
  - —Endpoint threat model similar to Adobe Flash
- How do you execute this code on a server?
  - —Other RCE vulnerability in an exposed service
  - —Privilege escalation if already local

Understand How You'll Be Attacked



How To Talk To Executives About Vulnerability Management

Counting Stats Don’t Make Good Metrics



Control the Message

- Help execs understand what they need to know to protect their jobs
- Generate and present metrics that are consumable
  - This provides clarity into what you're doing to protect them
  - Helps measure progress over time
- GOAL: Help them make business decisions based on this information

Let’s Review!

- Vulnerability management is a business process.
- Queryable infrastructure is the fabric of good asset management.
- Perform prioritization based on threat intel and asset criticality.
- Help executives make business decisions supported by metrics about unmitigated risk.

Apply What You Have Learned Today

Change your ideology, become a participant!

- Identify and start tracking key metrics now, to help show trends later.
  - **Critical Metric!** Coverage, coverage, coverage!
- Look for intelligence sources which inform threat/exploitation details.
- Embrace an “application stack” approach to asset management.
  - Understand how software is developed and deployed within your organization.

Apply What You Have Learned In 3 Months

Begin outreach and develop relationships!

- Start providing relevant intelligence briefings to executives.
- Communicate priority based on how an exploit could be delivered.
  - **New Metric!** How are you reducing work by deprioritizing CVSS severity?
- Champion efforts with operations to improve asset management.
  - “How can we help?” – But with suggestions, resources, and budget.

Apply What You Have Learned In 6 Months

Become part of the operations process!

- Start leveraging CI/CD processes for patch deployment.
  - **Key Metric!** You are committing code, use build metrics to track issues.
- Leverage queryable infrastructure for real time asset inventory.
- Codify a new vulnerability remediation SLA based on internal priority.

THANK YOU!

Email: jzelonis@forrester.com

LinkedIn: https://www.linkedin.com/in/zelonis/

Twitter: @jz415