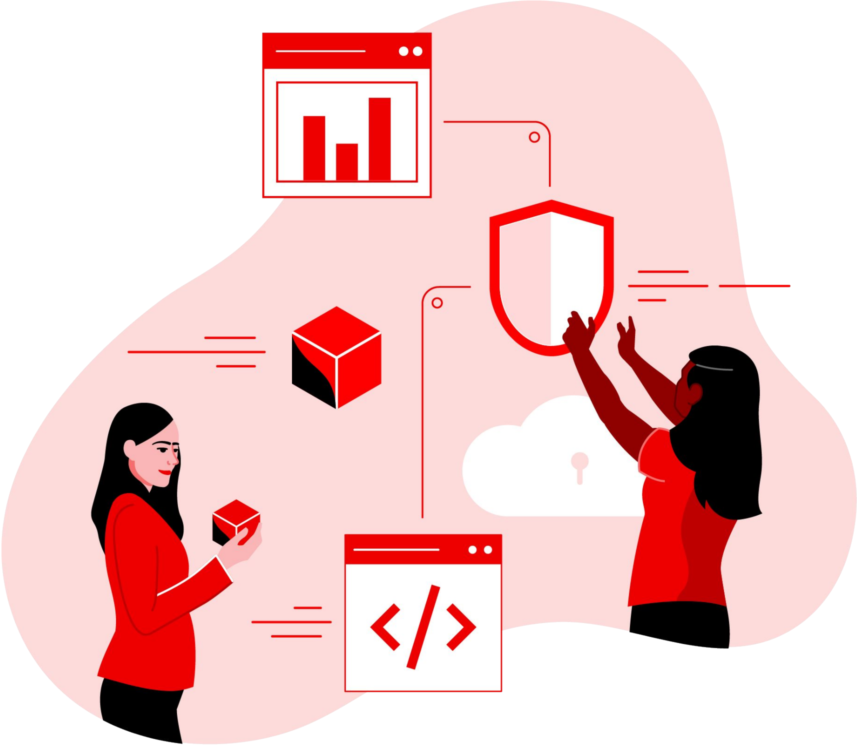
Red Hat | intel

Open Tour

Connecting people and solutions
to accelerate your business

Build a **trusted** software supply chain with Red Hat



Red Hat

2017

https://bit.ly/teachingelephants

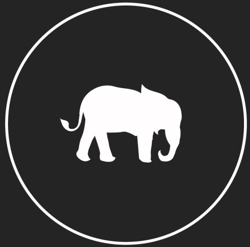
Teaching Elephants to Dance (and Fly!)

A DevOps Story

RED HAT DEVELOPERS

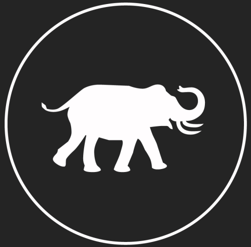
Digital Darwinism

The Developer’s Journey



Re-Org to
DevOps

Self-Service,
On-Demand,
Elastic
Infrastructure



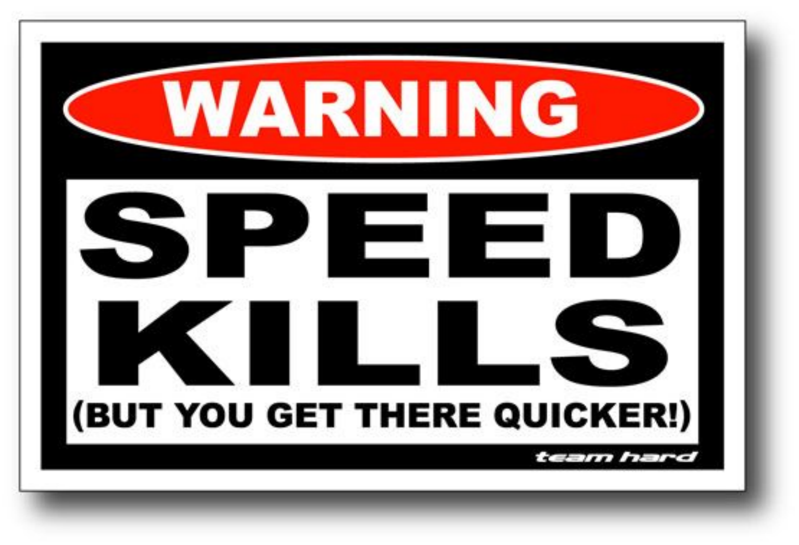
Automation
Puppet, Chef,
Ansible,
Kubernetes

CI & CD
Deployment
Pipeline

Advanced
Deployment
Techniques

Microservices
(and flying
elephants!)

‘Speed Kills!’ vs. ‘Go Fast, Go Safe’

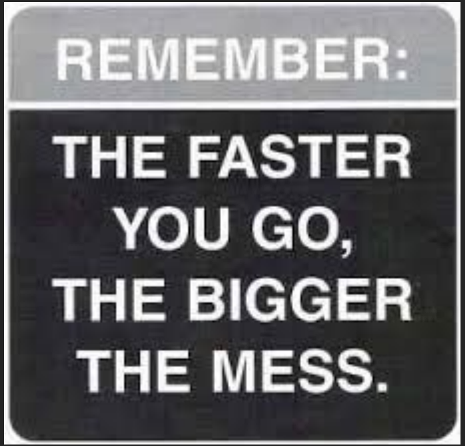


WARNING

SPEED KILLS

(BUT YOU GET THERE QUICKER!)

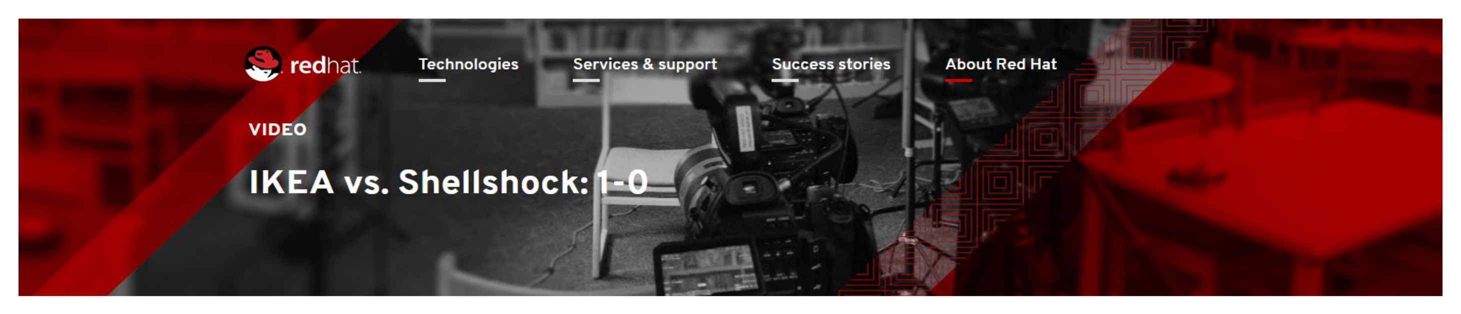
team hard



REMEMBER:

THE FASTER YOU GO, THE BIGGER THE MESS.

IKEA®



VIDEO

IKEA vs. Shellshock: 1-0

http://www.bbc.com/news/technology-29361794

https://www.redhat.com/en/about/videos/ikea-vs-shellshock

https://www.youtube.com/watch?v=aZA1JHMcd6I

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160

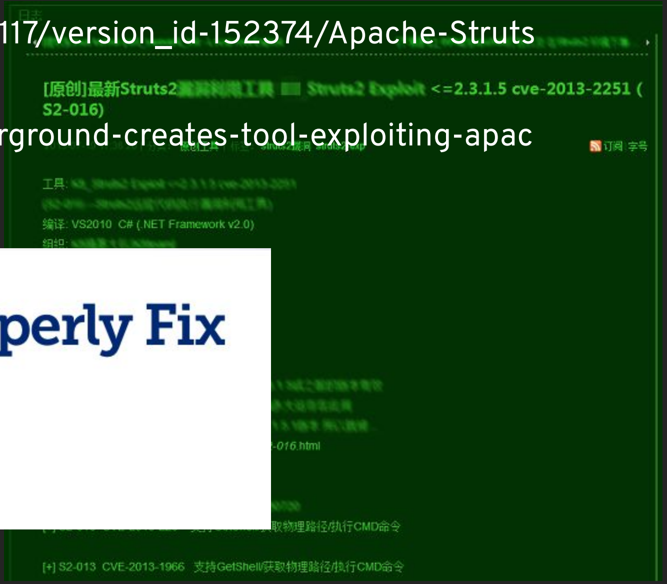
Actually, Slow Kills!

Slides from
Feb 2017
DevNexus

Apache Struts 2—zero-day vulnerability

https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-6117/version_id-152374/Apache-Struts-2.3.15.1.html

http://blog.trendmicro.com/trendlabs-security-intelligence/chinese-underground-creates-tool-exploiting-apache-struts-vulnerability/



[原创]最新Struts2[redacted] Struts2 Exploit <=2.3.1.5 cve-2013-2251 (S2-016)

订阅 字号

工具: [redacted]

编译: VS2010 C# (.NET Framework v2.0)

组织: [redacted]

-016.html

取物理路径/执行CMD命令

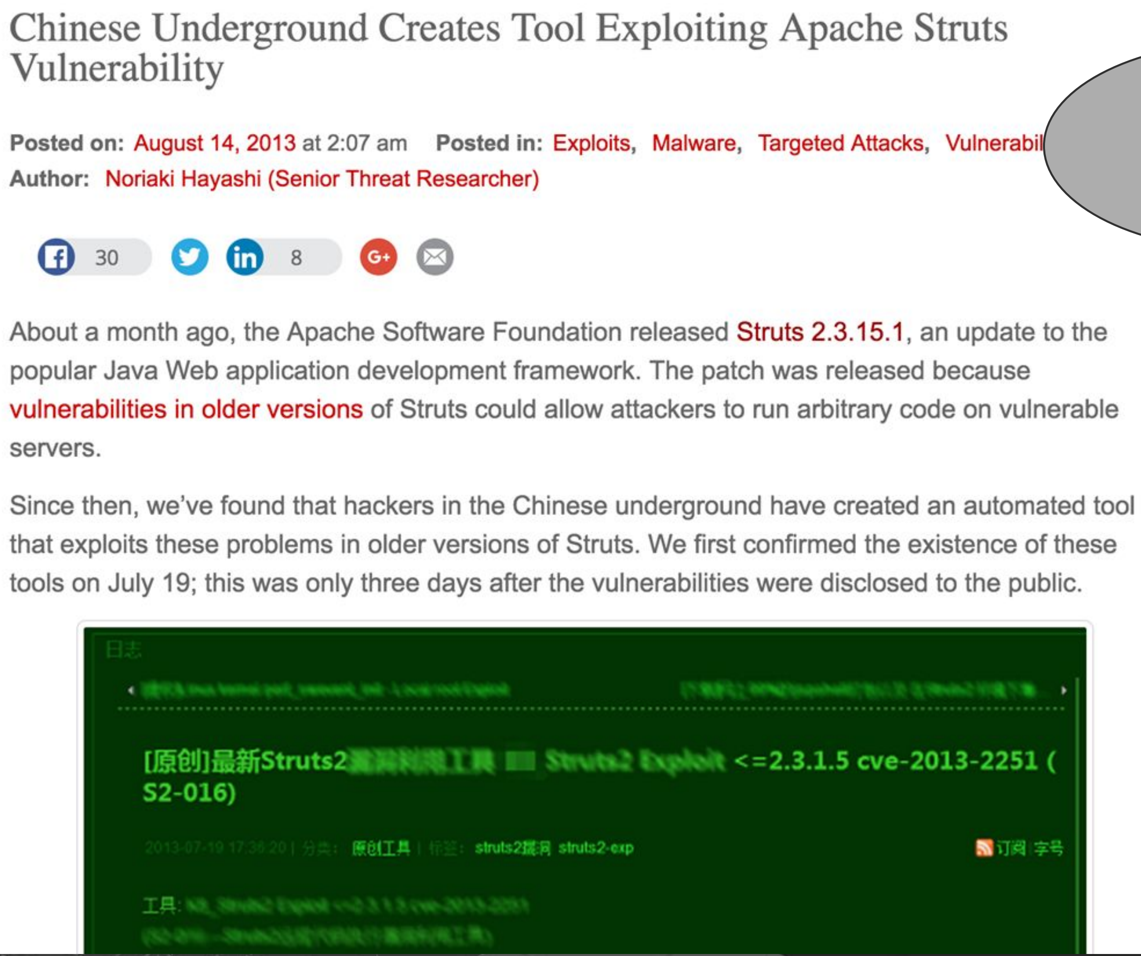
[+] S2-013 CVE-2013-1966 支持GetShell/获取物理路径/执行CMD命令

Apache Struts 2.3.16.2 Released to Properly Fix Zero-Day Vulnerability

Users are advised to update their installations as soon as possible

@burrsutter

RED HAT DEVELOPERS



Chinese Underground Creates Tool Exploiting Apache Struts Vulnerability

Posted on: August 14, 2013 at 2:07 am **Posted in:** Exploits, Malware, Targeted Attacks, Vulnerabil
Author: Noriaki Hayashi (Senior Threat Researcher)

30 8

About a month ago, the Apache Software Foundation released Struts 2.3.15.1, an update to the popular Java Web application development framework. The patch was released because vulnerabilities in older versions of Struts could allow attackers to run arbitrary code on vulnerable servers.

Since then, we've found that hackers in the Chinese underground have created an automated tool that exploits these problems in older versions of Struts. We first confirmed the existence of these tools on July 19; this was only three days after the vulnerabilities were disclosed to the public.

日志

[redacted] [redacted]

[原创]最新Struts2[redacted] <=2.3.1.5 cve-2013-2251 (S2-016)

2013-07-19 17:36:20 | 分类： 原创工具 | 标签： struts2漏洞 struts2-exp 订阅 字号

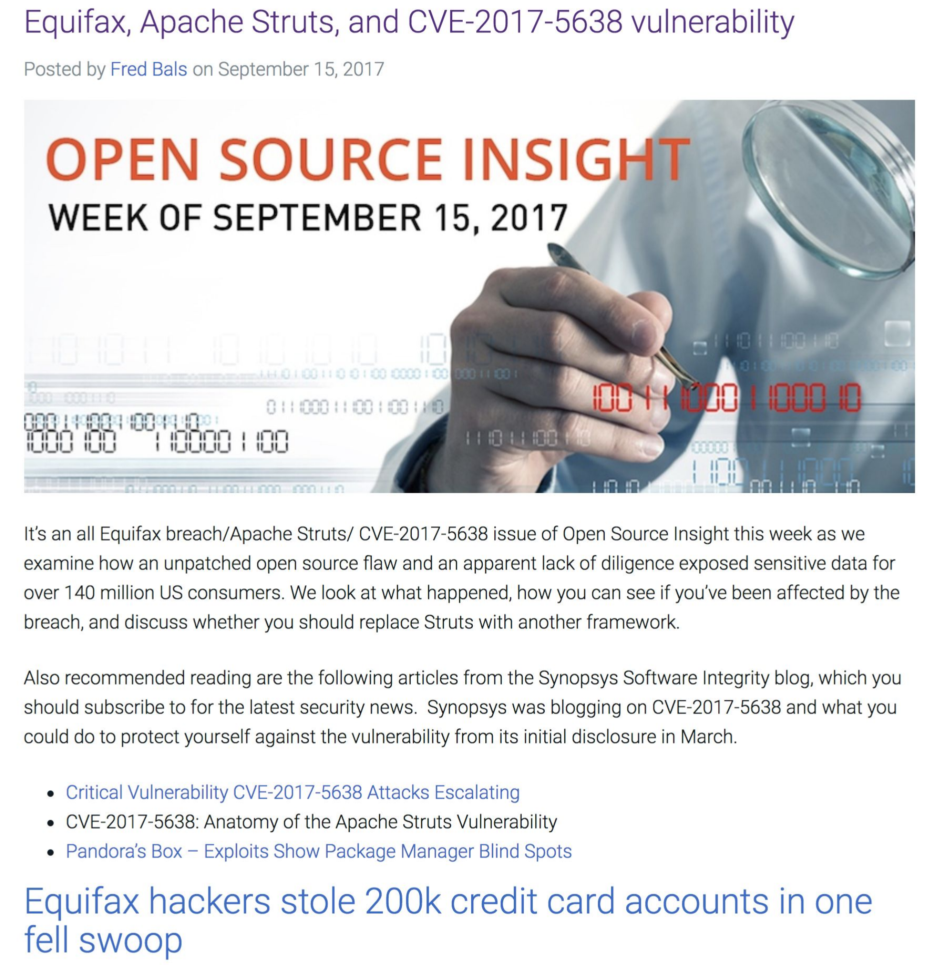
工具:[redacted]

Slides from
Feb 2017
DevNexus

And Then

"In September 2017, **Equifax** disclosed that a failure to patch one of its Internet servers against a pervasive software flaw — in a Web component known as **Apache Struts** — led to a breach that exposed personal data on 147 million Americans. "

KrebsonSecurity



Equifax, Apache Struts, and CVE-2017-5638 vulnerability

Posted by Fred Bals on September 15, 2017

OPEN SOURCE INSIGHT
WEEK OF SEPTEMBER 15, 2017

It's an all Equifax breach/Apache Struts/ CVE-2017-5638 issue of Open Source Insight this week as we examine how an unpatched open source flaw and an apparent lack of diligence exposed sensitive data for over 140 million US consumers. We look at what happened, how you can see if you've been affected by the breach, and discuss whether you should replace Struts with another framework.

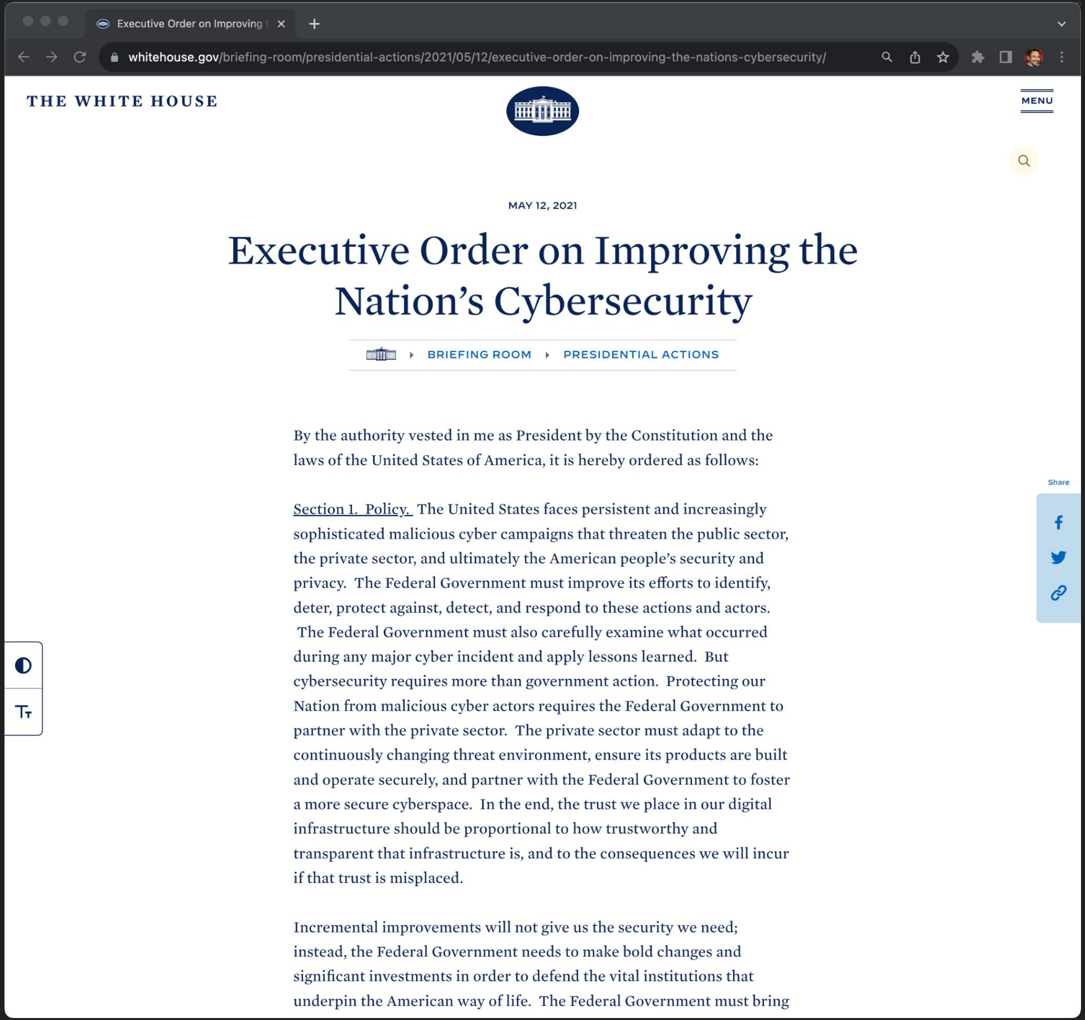
Also recommended reading are the following articles from the Synopsys Software Integrity blog, which you should subscribe to for the latest security news. Synopsys was blogging on CVE-2017-5638 and what you could do to protect yourself against the vulnerability from its initial disclosure in March.

- Critical Vulnerability CVE-2017-5638 Attacks Escalating
- CVE-2017-5638: Anatomy of the Apache Struts Vulnerability
- Pandora's Box – Exploits Show Package Manager Blind Spots

Equifax hackers stole 200k credit card accounts in one fell swoop

2021

May 2021
Cyber security
is
National security



Executive Order on Improving t
whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
THE WHITE HOUSE
MENU
BRIEFING ROOM
PRESIDENTIAL ACTIONS
Share

MAY 12, 2021

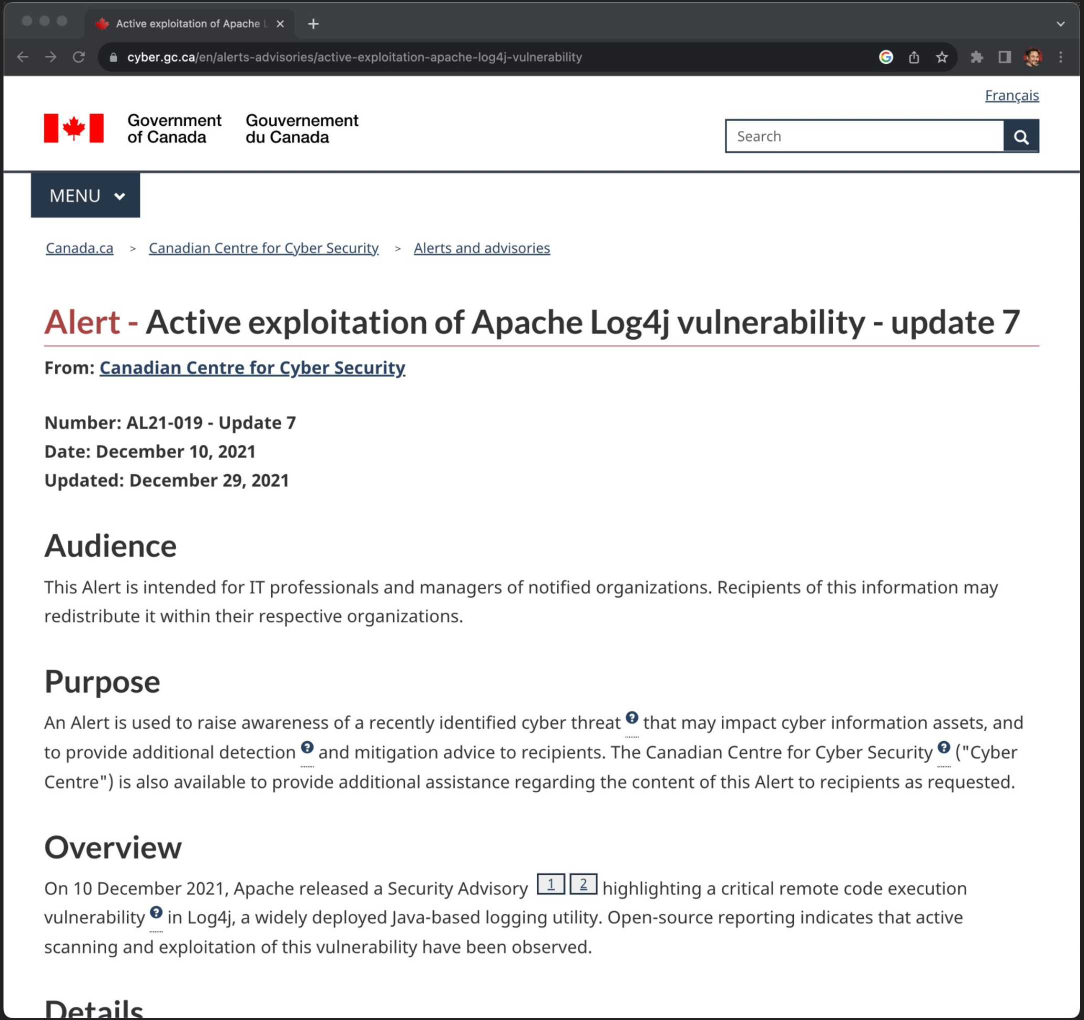
Executive Order on Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced.

Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life. The Federal Government must bring

December 2021
Log4Shell



Active exploitation of Apache L
cyber.gc.ca/en/alerts-advisories/active-exploitation-apache-log4j-vulnerability
Français
Government of Canada
Gouvernement du Canada
Search
MENU
Canada.ca > Canadian Centre for Cyber Security > Alerts and advisories

Alert - Active exploitation of Apache Log4j vulnerability - update 7

From: Canadian Centre for Cyber Security

Number: AL21-019 - Update 7
Date: December 10, 2021
Updated: December 29, 2021

Audience

This Alert is intended for IT professionals and managers of notified organizations. Recipients of this information may redistribute it within their respective organizations.

Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients. The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

Overview

On 10 December 2021, Apache released a Security Advisory [1] [2] highlighting a critical remote code execution vulnerability in Log4j, a widely deployed Java-based logging utility. Open-source reporting indicates that active scanning and exploitation of this vulnerability have been observed.

Details

Present Day

Open Tour Stockholm

Why you need a trusted software supply chain

Software supply chain attacks: a matter of when, not if

Ransom paid but a mere fraction to the overall downtime and recovery costs of a data breach

742%

average annual increase in software supply chain attacks over the past 3 years[1]

45%

of organizations worldwide will experience supply chain attacks by 2025[2]

1 in 5

data breaches are due to a software supply chain compromise[3]

71%

YoY increase in cost of average ransom payment[4]

[1] State of the Software Supply Chain | [2] 7 Top Trends in Cybersecurity for 2022 | [3] Cost of a Data Breach 2022 - IBM Report | [4] Average Ransom Payment Up 71% This Year, Approaches $1 Million |

First step: Adopting a DevSecOps mindset is essential

Built over an enterprise open source foundation to protect the software factory

55% DevSecOps leaders agree that a culture of shared ownership between application development and security teams is critical[1]

78% have initiatives that increase collaboration between DevOps and Security teams[2]

92% of IT leaders point out that enterprise open source solutions are important as their business accelerates application workloads to the open hybrid cloud[3]

[1] DevSecOps: Critical Risk Reduction Leads to Better Business Outcomes - IDC December 2021 | [2] State of Kubernetes Security Report 2022 - Red Hat Report | [3] State of Enterprise Open Source 2022 - Red Hat Report

But current approaches to scale DevSecOps are falling short

94% of tech leaders say that selecting the right security tools for their DevOps teams is challenging[1]

Overburdened with limited security expertise to keep pace with releases

Siloed teams lacking in integrated workflows, standardized security tools

Tool sprawl, context switching results in fragmented visibility

[1] DevSecOps: Critical Risk Reduction Leads to Better Business Outcomes - IDC December 2021

Recognize that open source software has eaten the world

Security of open source software has to be a fundamental, ongoing aspect of the SDLC

2 out of 3

organizations are already using OSS to augment internal development of new applications [1]

600$^{\text{est}}$

number of open source components in any given software, in codebases that are widely open source based[2]

90+$^{\%}$

of codebases contain open source components with no development activity or security fixes in two years[3]

[1]Better Together: DevOps and Open Source Go Hand in Hand - IDC Perspective, 2022 | [2] Open Source Security and Risk Analysis Report 2023 - Synopsys Report | [2]Open Source Security and Risk Analysis Report 2023

Catch application releases with security vulnerabilities

45% say software is released without going through security checks and/or testing[1].

- 3 of 5 organizations indicate their developers are using separate security tools[2].
- 65% of developers identified image scanning and vulnerability management as an important security use case[3].
- Over half of customers surveyed insist their developers use validated images[4].

[1][2] Walk the Line: GitOps and Shift Left Security - ESG Report | [3][4] State of Kubernetes Security Report 2022 - Red Hat Report

Account for all packaged components, dependencies

6 out of 7 project vulnerabilities come from transitive dependencies [1]

- Of the **1.2 billion** dependencies downloaded each month, **62%** had a transitive vulnerability[2]
- **73%** of organizations increased efforts to secure open source software only after an attack[3].
- **60%** of organizations will mandate Software Bill of Materials (SBOMs) by 2025[4]

[1][2] State of the Software Supply Chain - Sonotype Report | [3] Walk the Line: GitOps and Shift Left Security - ESG Report | [4] Gartner Report: Innovation Insight for SBOMs

Isolate critical alerts from the noise in real-time

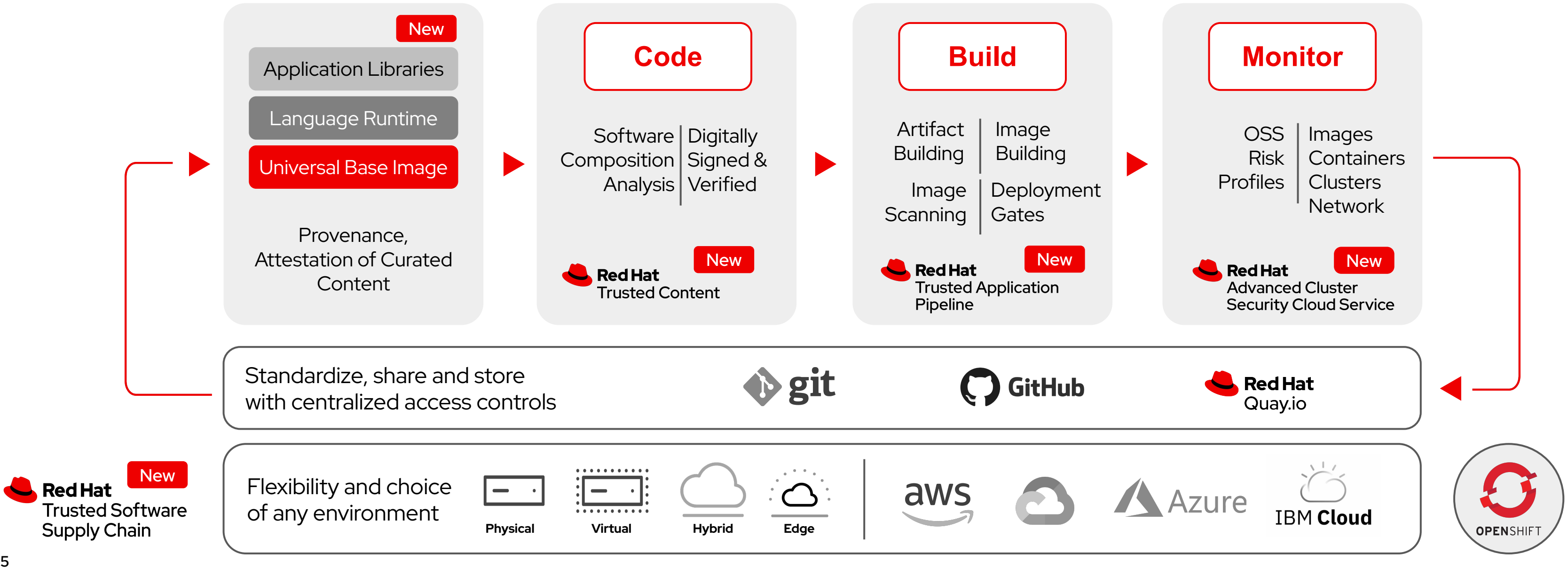
57% of surveyed worry the most about their runtime phase - for Day 2 operations[1]

- Nearly **53%** of respondents have experienced a misconfiguration incident in last 12 months[2].
- **83%** say they are experiencing an increase in IaC template misconfigurations[3].
- But only **28%** say they are scanning production environments for misconfigurations[4].

[1][2]State of Kubernetes Security Report 2022 - Red Hat Report | [3][4] Walk the Line: GitOps and Shift Left Security - ESG Report

Code, build, and monitor to a Trusted Software Supply Chain

*Delivered as a **cloud service** with integrated security guardrails at every phase of the software development lifecycle*



New

Application Libraries

Language Runtime

Universal Base Image

Provenance, Attestation of Curated Content

Code

Software Composition Analysis | Digitally Signed & Verified

New

Red Hat Trusted Content

Build

Artifact Building | Image Building

Image Scanning | Deployment Gates

New

Red Hat Trusted Application Pipeline

Monitor

OSS Risk Profiles | Images Containers Clusters Network

New

Red Hat Advanced Cluster Security Cloud Service

Standardize, share and store with centralized access controls

git | GitHub | Red Hat Quay.io

Red Hat Trusted Software Supply Chain New

Flexibility and choice of any environment

Secure the use of source code and transitive dependencies

Software supply chain security considerations for the software development lifecycle

Prevent & identify malicious **code**

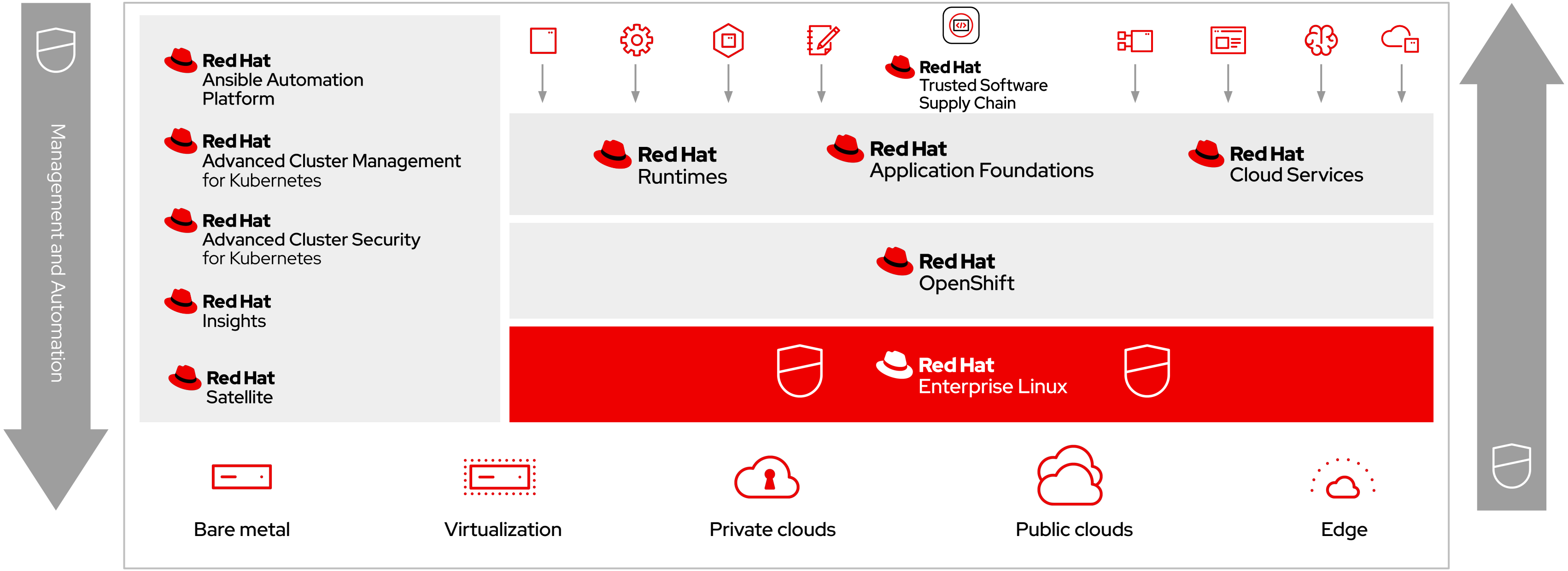
Safeguard **build** systems early

Continuously **monitor** security at runtime

Code, build, and monitor to a Trusted Software Supply Chain

Layered security throughout the stack and lifecycle

Build, deploy, and run applications on top of a hybrid cloud using DevSecOps practices


Management and Automation
Red Hat Ansible Automation Platform
Red Hat Advanced Cluster Management for Kubernetes
Red Hat Advanced Cluster Security for Kubernetes
Red Hat Insights
Red Hat Satellite
Red Hat Trusted Software Supply Chain
Red Hat Runtimes
Red Hat Application Foundations
Red Hat Cloud Services
Red Hat OpenShift
Red Hat Enterprise Linux
Bare metal
Virtualization
Private clouds
Public clouds
Edge

Enhance and extend security functionality

Build on Red Hat functionality through our **security partners** to better secure the entire DevOps life cycle.

- Increase Trust
- Reduce Risk
- Improve Compliance
- Enhance Collaboration
- Increase Agility
- Improve Quality

Application analysis	Identity & access management
SAST, SCA, IAST, DAST, Image risk	Authn, Authz, Secrets Vault, HSM, Provenance
Compliance	**Network controls**
Regulatory compliance, PCI-DSS, GDPR	CNI plugins, policies, traffic controls, service mesh
Data controls	**Runtime analysis & protection**
Data protection and encryption	RASP, production analysis
Audit and monitoring	**Remediation**
Logging, visibility, forensics	SOAR, automatic resolution

CYBERARK sysdig aqua SYNOPSYS TIGERA paloalto NETWORKS

NeuVector snyk anchore THALES portshift tufin

TREND MICRO IBM Lacework StackRox

Red Hat platform security

Secure host, container platform, namespace isolation, k8s and container hardening

Sign up today

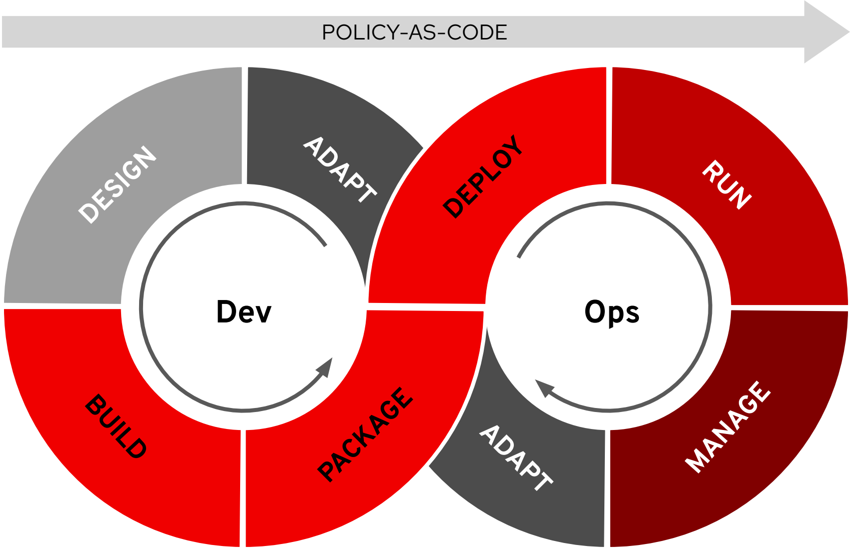
- Choose Red Hat for your trusted software supply chain + DevSecOps
- Learn how Red Hat Trusted Software Supply Chain can help: **red.ht/trusted**

Thank you

Red Hat Advanced Cluster Security: Use Cases

Security across the entire application lifecycle

- ➢ Image scanning
- ➢ Host scanning
- ➢ Serverless scanning
- ➢ Configuration scanning
- ➢ Compliance checks, auditing, reporting, remediation
- ➢ CI/CD integration and automation
- ➢ Artifact attestation



- ➢ Runtime threat detection
  - ✓ Process allowlisting
  - ✓ Anomaly detection
  - ✓ Policy-based detection
- ➢ Runtime vulnerability management
- ➢ Incident response
- ➢ Integrations
  - ✓ SIEM
  - ✓ Registries, CI/CD, runtimes, notification tools
- ➢ Feedback loop

VISIBILITY (images, deployments, network flows, processes, secrets use)

CONTAINERS AND K8S (on-premises, cloud/hybrid, edge)