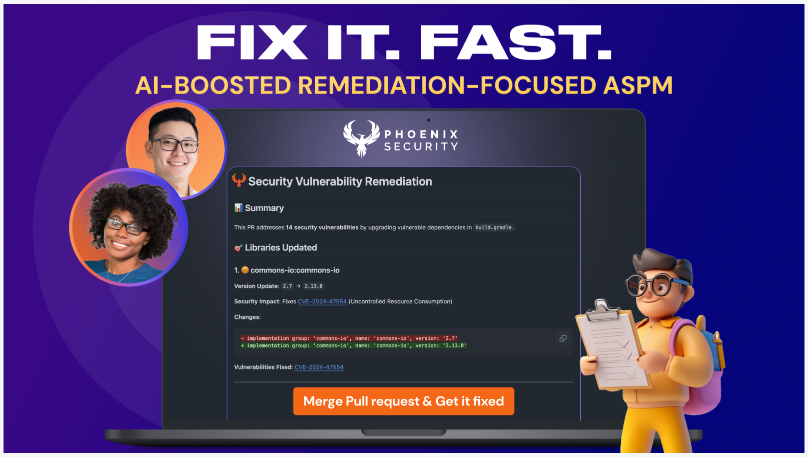
EINPRESSWIRE

Phoenix Security AI Agents Deliver Direct Remediation in GitHub From Single-Line Fixes to Full Build File Remediation

Redefining ASPM into ASM with remediation embedded: AI Agents That Don’t Just Identify Vulnerabilities, They Fix Them.

WASHINGTON, DC, UNITED STATES, November 6, 2025 /EINPresswire.com/ -- Redefining ASPM Application Security Vulnerability Management: AI Agents That Don’t Just Identify Vulnerabilities — They Fix Them.


FIX IT. FAST.
AI-BOOSTED REMEDIATION-FOCUSED ASPM
PHOENIX SECURITY
Merge Pull request & Get it fixed

Security Vulnerability Remediation

📊 Summary

This PR addresses **14 security vulnerabilities** by upgrading vulnerable dependencies in `build.gradle`.

🎯 Libraries Updated

1. 🟠 commons-io:commons-io

Version Update: `2.7` → `2.13.0`

Security Impact: Fixes CVE-2024-47554 (Uncontrolled Resource Consumption)

Changes:

```
- implementation group: 'commons-io', name: 'commons-io', version: '2.7'
+ implementation group: 'commons-io', name: 'commons-io', version: '2.13.0'
```

Vulnerabilities Fixed: CVE-2024-47554

Agent Autofix Remediation Phoenix Security

Phoenix Security, the leader in ASPM application security vulnerability management, announced today at OWASP Global Application Security DC the early availability of its latest AI innovation - the Phoenix Autofix Remediator Agent.

> “
> Our Remediator Agent doesn’t just tell you what’s broken; it tells who should fix what and where, why it's important, if it’s going to break the flow, adelivering what to fix to who needs it.”
>
> *Francesco Cipollone CEO & Co-Founder*

Built to work hand-in-hand with developers, the Remediator brings AI-powered, context-aware plans or fixes directly into GitHub, giving teams the choice to patch a single dependency, an entire chain of libraries, or rewrite a full build file - all with automated impact analysis and breaking-change assessment.

With this release, Phoenix Security’s AI agents move beyond research and contextual analysis - they now fix vulnerabilities directly in code, aligning remediation speed with DevSecOps and code-to-cloud security workflows.

“The goal was never to automate people out of the loop, but to give them a trusted co-pilot that understands risk, business impact, and context,” said Francesco Cipollone, CEO & Co-Founder of Phoenix Security. “Our Remediator Agent doesn’t just tell you what’s broken — it tells who should fix what and where, why it's important, if it’s going to break the flow, and delivers the fixes directly in the hands of engineering teams. The objective is to give teams flexibility to work in the way they want — with autofix or suggested remediation.”

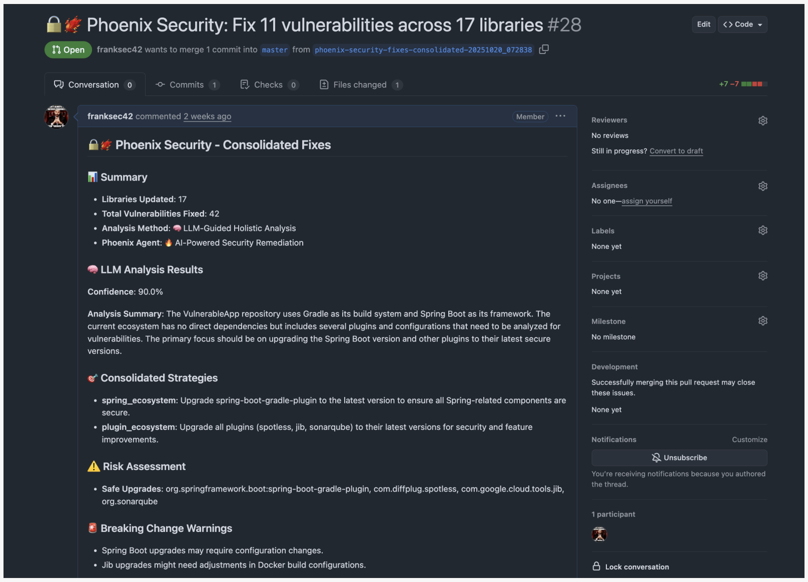
AI Remediation in Action: Fix Directly in GitHub

The Phoenix Remediator Agent integrates natively with GitHub, enabling automated PR creation and contextual autofix generation. Developers can now review, approve, or merge AI-proposed fixes with full transparency. The agent supports:
- Single dependency fixes — resolve isolated vulnerabilities with minimal code change.
- Chained dependency updates — tackle multi-layered vulnerabilities across dependent libraries.
- Full build file regeneration — generate a clean, validated replacement build file when vulnerabilities are systemic.
- Breaking change prediction — evaluate dependency upgrades and propose minimal paths to stability.
- Remediation plans — for complex issues, generate structured, context-aware plans rather than auto-commits.

Three Agents, One Mission: Precision From Research to Fix

Phoenix’s AI-powered agent architecture brings together three synergistic components:

The Researcher (GA)



🔒 Phoenix Security: Fix 11 vulnerabilities across 17 libraries #28

Open franksec42 wants to merge 1 commit into `master` from `phoenix-security-fixes-consolidated-20251020_072838`

franksec42 commented 2 weeks ago · Member

🔒 **Phoenix Security - Consolidated Fixes**

📊 **Summary**

- **Libraries Updated**: 17
- **Total Vulnerabilities Fixed**: 42
- **Analysis Method:** 🧠 LLM-Guided Holistic Analysis
- **Phoenix Agent**: 🔥 AI-Powered Security Remediation

🧠 **LLM Analysis Results**

Confidence: 90.0%

Analysis Summary: The VulnerableApp repository uses Gradle as its build system and Spring Boot as its framework. The current ecosystem has no direct dependencies but includes several plugins and configurations that need to be analyzed for vulnerabilities. The primary focus should be on upgrading the Spring Boot version and other plugins to their latest secure versions.

🎯 **Consolidated Strategies**

- **spring_ecosystem**: Upgrade spring-boot-gradle-plugin to the latest version to ensure all Spring-related components are secure.
- **plugin_ecosystem**: Upgrade all plugins (spotless, jib, sonarqube) to their latest versions for security and feature improvements.

⚠️ **Risk Assessment**

- **Safe Upgrades:** org.springframework.boot:spring-boot-gradle-plugin, com.diffplug.spotless, com.google.cloud.tools.jib, org.sonarqube

🚨 **Breaking Change Warnings**

- Spring Boot upgrades may require configuration changes.
- Jib upgrades might need adjustments in Docker build configurations.

Reviewers: No reviews. Still in progress? Convert to draft

Assignees: No one—assign yourself

Labels: None yet

Projects: None yet

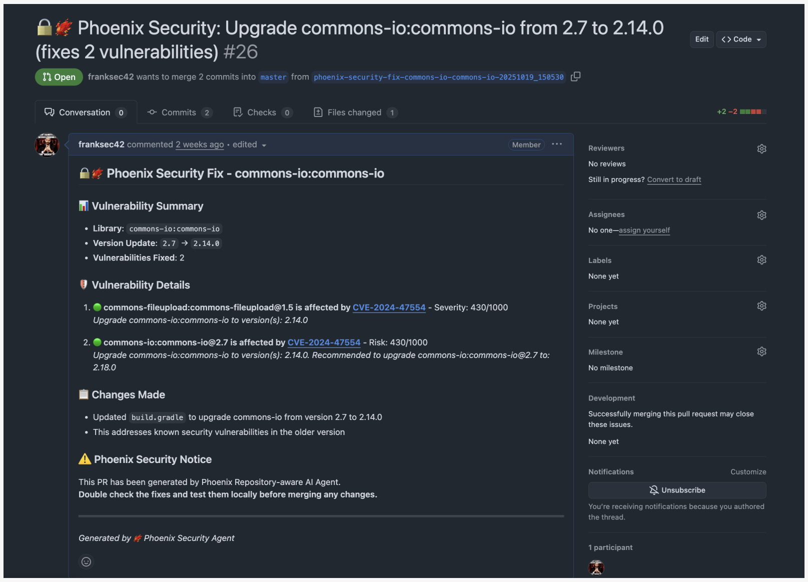
Milestone: No milestone

Development: Successfully merging this pull request may close these issues. None yet

Notifications: You’re receiving notifications because you authored the thread.

1 participant

AutoFix Agent Per Build File Fix



🔒 Phoenix Security: Upgrade commons-io:commons-io from 2.7 to 2.14.0 (fixes 2 vulnerabilities) #26

Open franksec42 wants to merge 2 commits into `master` from `phoenix-security-fix-commons-io-commons-io-20251019_150530`

franksec42 commented 2 weeks ago • edited · Member

🔒 **Phoenix Security Fix - commons-io:commons-io**

📊 **Vulnerability Summary**

- **Library**: `commons-io:commons-io`
- **Version Update**: `2.7` → `2.14.0`
- **Vulnerabilities Fixed**: 2

🛡 **Vulnerability Details**

1. 🟢 **commons-fileupload:commons-fileupload@1.5 is affected by CVE-2024-47554** - Severity: 430/1000
   Upgrade commons-io:commons-io to version(s): 2.14.0
2. 🟢 **commons-io:commons-io@2.7 is affected by CVE-2024-47554** - Risk: 430/1000
   Upgrade commons-io:commons-io to version(s): 2.14.0. Recommended to upgrade commons-io:commons-io@2.7 to: 2.18.0

📋 **Changes Made**

- Updated `build.gradle` to upgrade commons-io from version 2.7 to 2.14.0
- This addresses known security vulnerabilities in the older version

⚠️ **Phoenix Security Notice**

This PR has been generated by Phoenix Repository-aware AI Agent.
Double check the fixes and test them locally before merging any changes.

Generated by Phoenix Security Agent

Reviewers: No reviews. Still in progress? Convert to draft

Assignees: No one—assign yourself

Labels: None yet

Projects: None yet

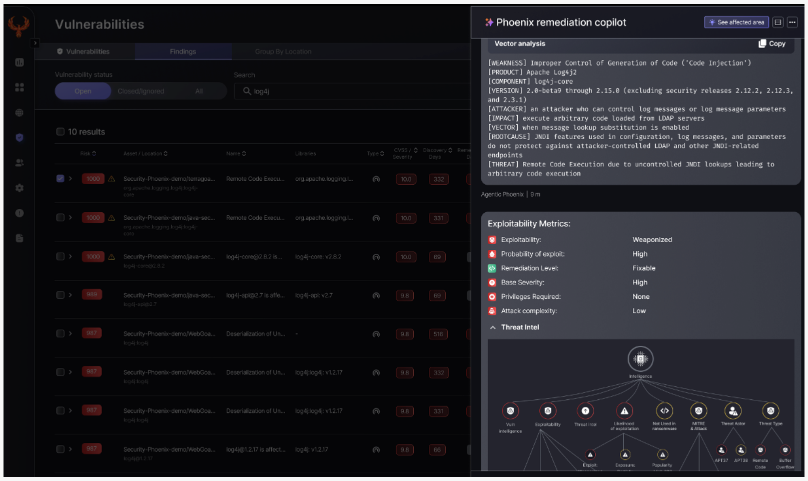
Milestone: No milestone

Development: Successfully merging this pull request may close these issues. None yet

Notifications: You’re receiving notifications because you authored the thread.

1 participant

PR for library from Phoenix Security ASPM remediator agent



Vector analysis

```
[WEAKNESS] Improper Control of Generation of Code ('Code Injection')
[PRODUCT] Apache Log4j2
[COMPONENT] log4j-core
[VERSION] 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3,
and 2.3.1)
[ATTACKER] an attacker who can control log messages or log message parameters
[IMPACT] execute arbitrary code loaded from LDAP servers
[VECTOR] when message lookup substitution is enabled
[ROOTCAUSE] JNDI features used in configuration, log messages, and parameters
do not protect against attacker-controlled LDAP and other JNDI-related
endpoints
[THREAT] Remote Code Execution due to uncontrolled JNDI lookups leading to
arbitrary code execution
```

Agentic Phoenix | 9 m

Exploitability Metrics:

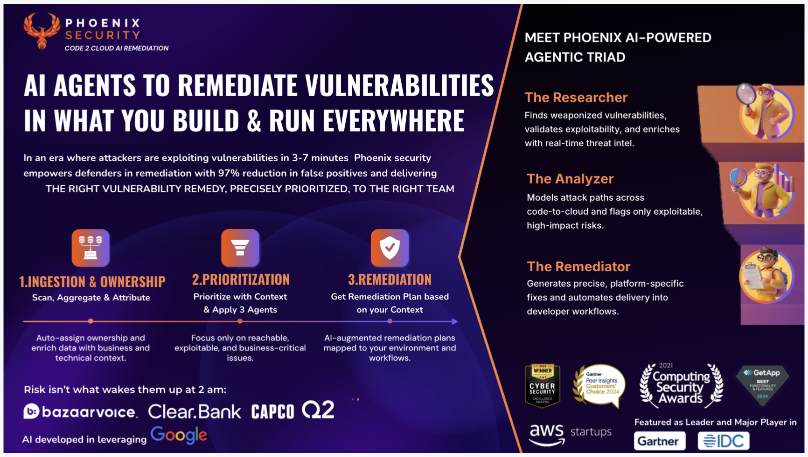
Exploitability:	Weaponized
Probability of exploit:	High
Remediation Level:	Fixable
Base Severity:	High
Privileges Required:	None
Attack complexity:	Low

Threat Intel

AI Agent Analyzer Phoenix Security

Continuously monitors threat intelligence feeds, mapping vulnerabilities to MITRE ATT&CK, CWE, and ransomware campaigns — powered by proprietary models developed with Google Cloud.

The Analyzer
Uses Phoenix's code-to-cloud reachability and STRIDE threat modeling to reveal exactly how a vulnerability impacts a business service or application.



PHOENIX SECURITY
CODE 2 CLOUD AI REMEDIATION

AI AGENTS TO REMEDIATE VULNERABILITIES IN WHAT YOU BUILD & RUN EVERYWHERE

In an era where attackers are exploiting vulnerabilities in 3-7 minutes Phoenix security empowers defenders in remediation with 97% reduction in false positives and delivering
THE RIGHT VULNERABILITY REMEDY, PRECISELY PRIORITIZED, TO THE RIGHT TEAM

1.INGESTION & OWNERSHIP
Scan, Aggregate & Attribute
Auto-assign ownership and enrich data with business and technical context.

2.PRIORITIZATION
Prioritize with Context & Apply 3 Agents
Focus only on reachable, exploitable, and business-critical issues.

3.REMEDIATION
Get Remediation Plan based on your Context
AI-augmented remediation plans mapped to your environment and workflows.

Risk isn't what wakes them up at 2 am:

AI developed in leveraging Google

MEET PHOENIX AI-POWERED AGENTIC TRIAD

The Researcher
Finds weaponized vulnerabilities, validates exploitability, and enriches with real-time threat intel.

The Analyzer
Models attack paths across code-to-cloud and flags only exploitable, high-impact risks.

The Remediator
Generates precise, platform-specific fixes and automates delivery into developer workflows.

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS
Gartner Peer Insights Customers' Choice 2024
2021 Computing Security Awards
GetApp BEST FUNCTIONALITY & FEATURES 2024
aws startups

Featured as Leader and Major Player in Gartner IDC

Agents Remediation Main Phoenix Security Agentic AI

The Remediator (New)
Moves context into action with a remediation plan in reports and code pushed directly to GitHub, translating all intelligence into real, executable change. Using reachability, contextual deduplication, and lineage data, it generates environment-specific autofixes, remediation campaigns, and Jira or ServiceNow remediation plans — or commits changes directly to GitHub.

Together, they transform vulnerability management from "find and report" to "analyze and fix," cutting remediation time from weeks to minutes.

- AI Fixes That Understand Context: This capability is built on Phoenix's proven Contextual ASPM Engine, combining:
- Reachability Analysis – Removes non-exploitable vulnerabilities, reducing noise by 91%.
- Contextual Deduplication – Prevents duplicate findings across code, containers, and runtime.
- Container Version Control – Tracks lineage for precise remediation paths.
- 4D Risk Formula – Balances exploitability, exposure, and business impact for risk-based prioritization.

AI fixes aren't just applied—they're validated in real-world deployment contexts, advancing the state of ASPM application security vulnerability management.

Proven Results Across Industries

- ClearBank Case Study cut container noise by 98%, eliminated up to 99% of criticals, and saved $2.6M in analyst time annually—equivalent to 4 hours per security engineer per week.
- Bazaarvoice eradicated all critical vulnerabilities in two weeks and reduced high-risk findings by 40%, creating immediate alignment between security and engineering.
- An Ad-tech enterprise achieved a 78% reduction in container vulnerabilities while unifying code-to-cloud security visibility.

Human-Aligned AI: Fix Faster, Stay in Control

Unlike generic LLM copilots, Phoenix Security’s AI Agents are purpose-built for application security. Every action is traceable, reviewable, and aligned to the business context. Teams decide when to apply fixes automatically, when to review, or when to generate compensating controls.

Security remains in command — AI eliminates the manual grind.

Availability

- Researcher Agent — Generally Available
- Remediator Agent with AI Autofix in GitHub — Rolling out globally through Q4 2025–Q1 2026
- Analyzer Agent — Q2 2026

For demos or early access to the AI Autofix capabilities, visit Phoenix Security

Phil Moroni
Phoenix Security
+1 919-594-8888
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X