

# AWS's Log4Shell Hot Patch Container Escape and Priv

65,754 people reacted

👍 62

7 min. read



By Yuval Avrahami

April 19, 2022 at 3:00 PM

Category: Cloud, Vulnerability

Tags: Apache Log4j, AWS, container escape, containers, CVE-2022-0070, CVE-2022-0071, log4j, privilege escalation

This post is also available in: [日本語 \(Japanese\)](#)

## Executive Summary

Following [Log4Shell](#), AWS released several [hot patch solutions](#) that monitor for vulnerable Java applications and Java [containers](#) and patch them on the fly. Each solution suits a different environment, covering standalone servers, Kubernetes clusters, Elastic Container Service (ECS) clusters and Fargate. The hot patches aren't exclusive to AWS environments and can be installed onto any cloud or on-premises environment.

Unit 42 researchers identified severe security issues within these patching solutions and partnered with

### 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

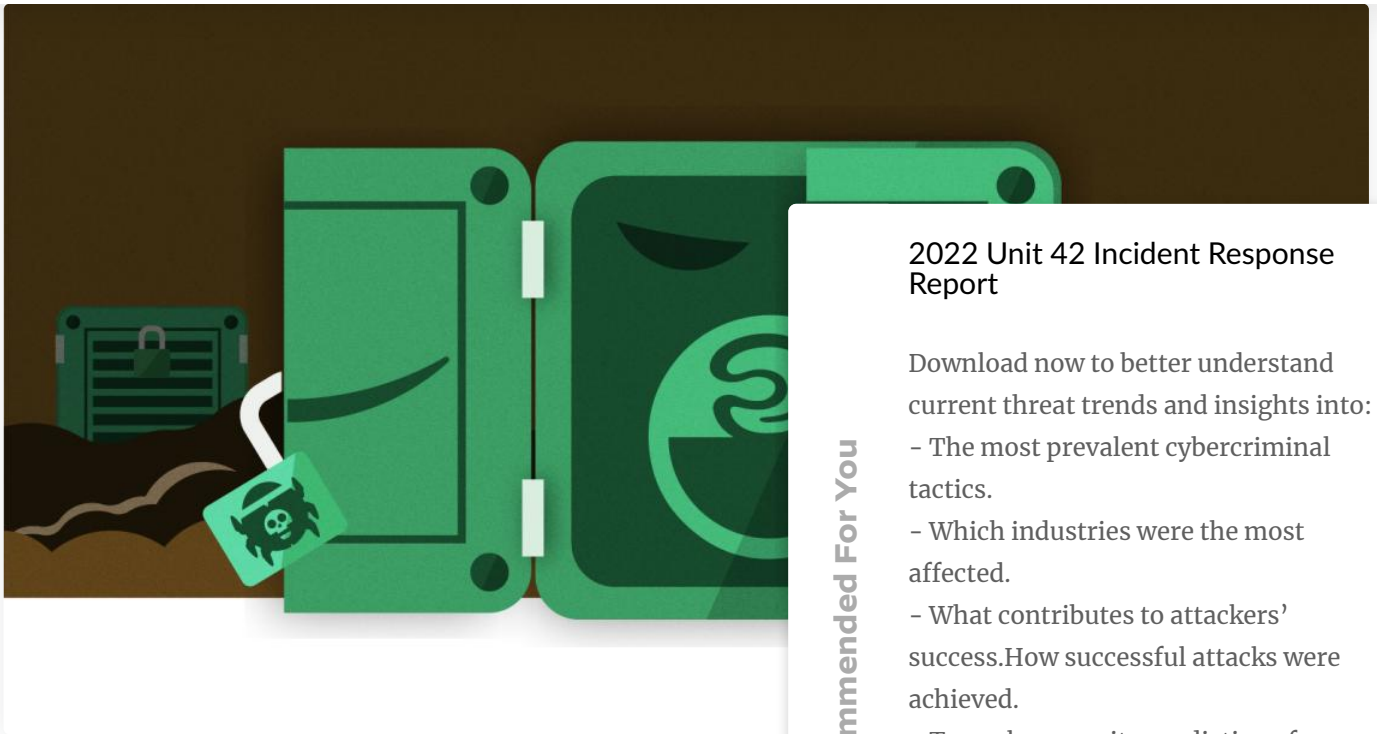
- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

**Manage My Cookie Settings**



Containers can escape regardless of whether they run Java. If the host runs [Bottlerocket](#), AWS's hardened Linux distribution for containers, namespaces or as a non-root user are affected as well. Unit 42 tracks CVE-2022-03101, CVE-2022-0070 and CVE-2022-0071 to track the vulnerability.

AWS released a fixed version for each hot patch solution on Dec. 17, 2021.

1. Version 1.1-16 of the `log4j-cve-2021-44228-hotpatch` [package](#), which bundles the hot patch service.
2. Version 1.1-16 of the `kubernetes-log4j-cve-2021-44228-node-agent` [Daemonset](#), which installs the updated package.
3. Version 1.02 of [Hotdog](#), a hot patch solution for Bottlerocket hosts based on Open Container Initiative (OCI) hooks.

Unit 42 advises anyone who installed any of these hot patches to upgrade to a fixed version. Note that starting from Dec. 17, 2021, JDK packages (Java installations) on Amazon Linux [automatically installed](#) the `log4j-cve-2021-44228-hotpatch` package. Alternatively, users who are confident their applications are patched against Log4Shell can disable the hot patch service following the instructions in the Mitigations section below.

## 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

**Manage My Cookie Settings**

# Table of Contents

[Overview of AWS Log4Shell Hot Patches](#)  
[Root Cause Analysis](#)  
[Container Escape Demo](#)  
[Impact](#)  
[Mitigations](#)  
[Safely Interacting With Containers](#)  
[Conclusion](#)  
[Additional Resources](#)  
[Disclosure Timeline](#)

## Overview of AWS Log4Shell

Log4Shell proved itself as one of the worst vulnerabilities of the year. As an issue at scale, AWS open-sourced several hot patch solutions. Hot patching is the process of injecting a fix to a vulnerable application as a short-term solution until a new, fixed version of the application is available.

AWS released three hot patching solutions that detect processes and containers running vulnerable Java applications and patch them on the fly:

1. A [hot patch service](#) bundled in an RPM package. Starting from Dec. 17, 2021, this service is automatically installed with Amazon Linux JDK (Java) packages. Fargate customers could've asked for this service to be installed on the hosts running their containers.
2. A [hot patch Daemonset](#) for Kubernetes clusters, which installs the aforementioned hot patch service on all nodes.
3. [Hotdog](#), a hot patch solution bundled as a set of OCI hooks. Hotdog is primarily intended for Bottlerocket hosts.

These solutions cover most compute environments, from Kubernetes clusters to ECS clusters, Fargate containers and standalone servers. They aren't exclusive to AWS environments, and can be installed onto other cloud environments or on-premises.

### 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

**Manage My Cookie  
Settings**

# Root Cause Analysis

AWS's hot patch solutions continuously search for Java processes and patch them against Log4Shell on the fly. Any process running a binary named "java" – inside or outside of a container – is considered a candidate for the hot patch.

To patch Java processes inside containers, the hot patch solution, for example, they run the container's "java" binary twice: once to patch and once to inject the hot patch. The issue was that they invoked container processes without the limitation. That is, the new processes would run without the limitation of container processes.

For example, the "java" binary was invoked in the container (excluding the user namespace). But aside from that, it was not isolated without the [isolation technologies that normally confine container processes](#). It also ran as the root user regardless of the container's user.

A malicious container therefore could have included a malicious hot patch solution into invoking it with elevated privileges and then abuse its elevated privileges to escape the container and run on the host. The hot patch solutions now properly containerize container binaries.

Aside from containers, the hot patch service also patched host processes. A malicious unprivileged process could have created and run a hot patch service into executing it with elevated privileges. The fixed hot patch service now spawns "java" binaries with the same privileges as the Java process being patched.

## Container Escape Demo

To verify the vulnerability is exploitable, we built a proof of concept (PoC) container image. When deployed to a cluster or VM that runs a vulnerable version of a hot patch solution, the container exploits the vulnerabilities to escape and gain root code execution on the underlying host. It then sends a [reverse shell](#) to an attacker-controlled server.

In the demo video below, a user installed the hot patch Daemonset to an EKS cluster. The demo then simulates a supply chain attack by showing what happens when the user inadvertently runs a malicious container image that exploits the hot patch.

### 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

**Manage My Cookie Settings**

## AWS Log4Shell Hot Patch Exploit Demo



*Video 1. CVE-2021-3100 exploit demo.*

While the demo showcases a supply chain attack, existing code (e.g., network payload) can also exploit the issues to escape and t... decided not to share the exploit's implementation details at weaponizing it.

## Impact

Given the urgency surrounding Log4Shell, users may have deployed hot patches at scale, inadvertently putting container environments at risk. Even after Java applications were patched against Log4Shell, users may have kept the hot patch running for defense-in-depth as there isn't a strong incentive to remove it.

Containers are often used as a security boundary between applications running on the same machine. A container escape allows an attacker to extend a campaign beyond a single application and compromise neighboring services. In Kubernetes clusters, a single container escape is unfortunately sometimes enough to take over the entire cluster.

The issues are exploitable regardless of the container configuration, so even environments that enable advanced isolation techniques like running containers in [user namespaces](#) or as a non-root user are affected.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

### 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

**Manage My Cookie Settings**

# Mitigations

AWS released a fix for each hot patch solution. Once a host runs a fixed version, container escape and privilege escalation are no longer possible.

1. In Kubernetes clusters, you can install the fixed hot patch provided by AWS. Note that only deleting the hot patch DaemonSet service from your nodes. **Updated April 25:** Currently, there are no fixed hot patch solutions for Debian-based hosts (Debian and Ubuntu). See this [GitHub](#) for more information. The fixed DaemonSet version for Debian-based hosts was released on April 25. The `log4j-cve-2021-44228-hotpatch` package is available for Debian-based hosts.
2. On standalone hosts, you can upgrade by running `yum update log4j-cve-2021-44228-hotpatch`.
3. Hotdog users need to upgrade to the [latest version](#).

Alternatively, if you're confident that your environment is protected by the hot patch service on a host by running `sudo touch /etc/hosts.allow` and `hotpatch.kill`. To disable Hotdog, run `apiclient set --hotdog-enabled=false`.

Prisma Cloud customers can identify affected hosts under their subscriptions. For more information on the hot patch packages and alerts customers on VMs running on Amazon Linux 2, use the Amazon Linux Security Advisories (ALAS-2021-1554, ALAS-2021-1732, ALAS-2022-1580 and ALAS-2022-1773).

## 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

### Get the report

Recommended For You

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

Manage My Cookie Settings

## 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

Recommended For You

**Get the report**

Figure 1. Prisma Cloud detects and alerts on vulnerable log4j

Palo Alto Networks [Prisma Cloud](#), [Cortex XDR](#) and [Next-Gen](#) follow-on attacker activities and disrupt command and control communications like the reverse shell used in the demo.

## Safely Interacting With Containers

CVE-2021-3100, CVE-2021-3101, CVE-2022-0070 and CVE-2022-0071 add to a long list of container escape vulnerabilities that arise from a host process directly interacting with a running container. Simple tasks like copying files or spawning a new containerized process can have surprising outcomes when the container is malicious.

If you're building software around containers, defer to an established container runtime like [runc](#) for operations involving a container's processes or filesystem. Although they have also had their share of vulnerabilities, container runtimes are by far the most vetted and mature programs for safely interacting with containers.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

**Manage My Cookie  
Settings**

as soon as possible. Multitenant container environments and clusters running untrusted images are especially at risk.

If you're still patching against Log4Shell, prioritize that effort first. While the presented issues can lead to severe attacks against container environments, Log4Shell has rightfully earned its spot as one of the worst vulnerabilities of all time and is still being actively exploited.

We'd like to thank AWS for their partnership and coordination in responding to these issues as efficiently as possible. As Log4Shell exploitation peaked, AWS's hot patch releases were a critical part of the response. With these vulnerabilities fixed, it's now possible to move forward with confidence while also keeping container environments secure.

## Additional Resources

- [Unit 42 analysis of Log4Shell](#)
- [AWS advice on mitigating Log4Shell in container environments](#)
- [Prisma Cloud Mitigations for Log4Shell](#)

## Disclosure Timeline

- **Dec. 14:** AWS releases hot patch package with support for affected versions.
- **Dec. 20:** Unit 42 researchers identify the issue.
- **Dec. 21:** Advisory sent to AWS.
- **Dec. 22:** AWS acknowledges the issue.
- **Dec. 23:** AWS releases fixes and advisories for affected components.
- **Dec. 27:** Unit 42 reports bypasses for the initial fixes to AWS.
- **Feb. 9:** Unit 42 researchers meet with AWS security to discuss fixes.
- **April 1:** AWS shares fixed versions for Unit 42 review.
- **April 4:** Unit 42 points out a few remaining issues.
- **April 19:** AWS releases final fixes and advisories; Unit 42 discloses the vulnerabilities publicly.

Updated May 5, 2022, at 11:10 a.m. PT.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

### 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

Manage My Cookie Settings



Sign up to receive the latest news, cyber threat intelligence and research from us

Email address

Subscribe



I'm not a robot

reCAPTCHA  
Privacy - Terms

By submitting this form, you agree to our [Terms of Use](#) and acknowledge



## Popular Resources

[Resource Center](#)

[Blog](#)

[Communities](#)

[Tech Docs](#)

[Unit 42](#)

[Sitemap](#)

## Legal Notices

[Privacy](#)

[Terms of Use](#)

[Documents](#)

## Account

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

## 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

**Manage My Cookie  
Settings**

## 2022 Unit 42 Incident Response Report

Download now to better understand current threat trends and insights into:

- The most prevalent cybercriminal tactics.
- Which industries were the most affected.
- What contributes to attackers' success. How successful attacks were achieved.
- Top cybersecurity predictions from our incident responders.
- Actionable recommendations to get ahead of future threats.

**Get the report**

Recommended For You

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

**Manage My Cookie  
Settings**