

Spring4Shell (CVE-2022-22965): details and mitigations

SL securelist.com/spring4shell-cve-2022-22965/106239/



[Incidents](#)

[Incidents](#)

04 Apr 2022

minute read



Authors



Last week researchers found the critical vulnerability CVE-2022-22965 in Spring – the open source Java framework. Using the vulnerability, an attacker can execute arbitrary code on a remote web server, which makes CVE-2022-22965 a critical threat, given the Spring framework’s popularity. By analogy with the [infamous Log4Shell threat](#), the vulnerability was named Spring4Shell.

CVE-2022-22965 and CVE-2022-22963: technical details

CVE-2022-22965 (Spring4Shell, SpringShell) is a vulnerability in the Spring Framework that uses data binding functionality to bind data stored within an HTTP request to certain objects used by an application. The bug exists in the *getCachedIntrospectionResults* method, which can be used to gain unauthorized access to such objects by passing their class names via an HTTP request. It creates the risks of data leakage and remote code execution when special object classes are used. This vulnerability is similar to the long-closed CVE-2010-1622, where class name checks were added as a fix so that the name did not match *classLoader* or *protectionDomain*. However, in a newer version of JDK an alternative method exists for such exploitation, for example, through Java 9 Platform Module System functionality.

So an attacker can overwrite the Tomcat logging configuration and then upload a JSP web shell to execute arbitrary commands on a server running a vulnerable version of the framework.

A vulnerable configuration consists of:

- JDK version 9+
- Apache Tomcat for serving the application
- Spring Framework versions 5.3.0 to 5.3.17 and 5.2.0 to 5.2.19 and below
- application built as a WAR file

CVE-2022-22963 is a vulnerability in the routing functionality of Spring Cloud Function that allows code injection through Spring Expression Language (SpEL) by adding a special *spring.cloud.function.routing-expression* header to an HTTP request. SpEL is a special expression language created for Spring Framework that supports queries and object graph management at runtime. This vulnerability can also be used for remote code execution.

A vulnerable configuration consists of:

Spring Cloud Function 3.1.6, 3.2.2 and older versions

Mitigations for Spring vulnerabilities exploitation

CVE-2022-22965 is fixed in 2.6.6; see [the Spring blog for details](#).

To fix CVE-2022-22963, you also need to install the new Spring Cloud Function versions; see the [VMware website for details](#).

To detect exploitation attempts, ensure that Advanced Exploit Prevention and Network Attack Blocker features are enabled. Some techniques used during exploitation can be seen in other exploits that we detect, which is why the verdict names can differ.

Indicators of Compromise

Verdicts

PDM:Exploit.Win32.Generic

UMIDS:Intrusion.Generic.Agent.gen

Intrusion.Generic.CVE-*. *

MD5 hashes of the exploits

7e46801dd171bb5bf1771df1239d760c – shell.jsp (CVE-2022-22965)

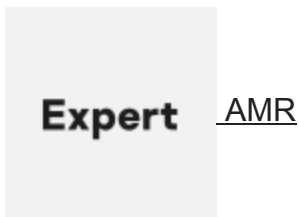
3de4e174c2c8612aebb3adef10027679 – exploit.py (CVE-2022-22965)

Detection of the exploitation process with Kaspersky EDR Expert

The screenshot shows the Kaspersky Anti Targeted Attack Platform interface. The left sidebar contains navigation options: Dashboard, Alerts, Threat Hunting, Tasks, Prevention, User roles, Storage, Endpoint Agents, Reports, and Settings. The main content area displays details for an event titled 'Spring4Shell_Lattack'. It includes fields for IOA name(s), Importance (High), Confidence (High), and TAA exclusions. Below this is a 'Description' section with a detailed technical explanation of the CVE-2022-22965 vulnerability. A 'Recommendations' section provides steps for host verification and patching. A 'MITRE Technique' table lists T1190 (Exploit Public-Facing Application) with its tactics and source reference. A 'Possible false positive' section notes that the detection is based on endpoint protection platform data.

- [Java](#)
- [Malware Descriptions](#)
- [Vulnerabilities and exploits](#)

Authors



Spring4Shell (CVE-2022-22965): details and mitigations

Your email address will not be published. Required fields are marked *



Table of Contents

- [CVE-2022-22965 and CVE-2022-22963: technical details](#)
- [Mitigations for Spring vulnerabilities exploitation](#)
- [Indicators of Compromise](#)

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm

17 Jun 2020, 1:00pm

26 Aug 2020, 2:00pm

22 Jul 2020, 2:00pm

Subscribe to our weekly e-mails

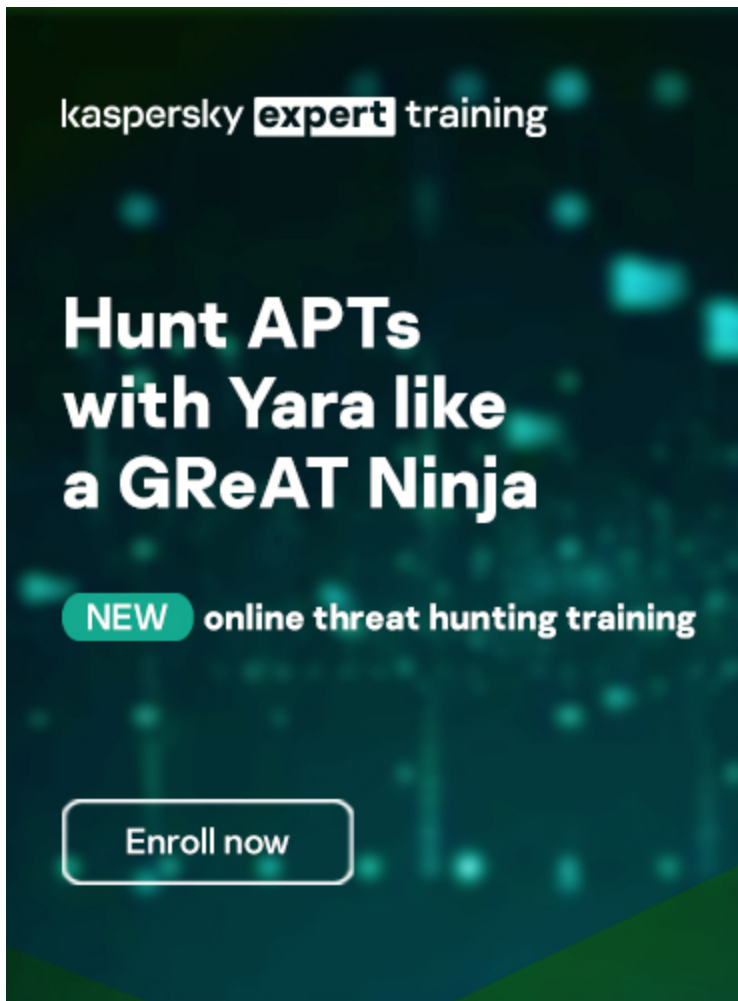
The hottest research right in your inbox

-

-

-

-



Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

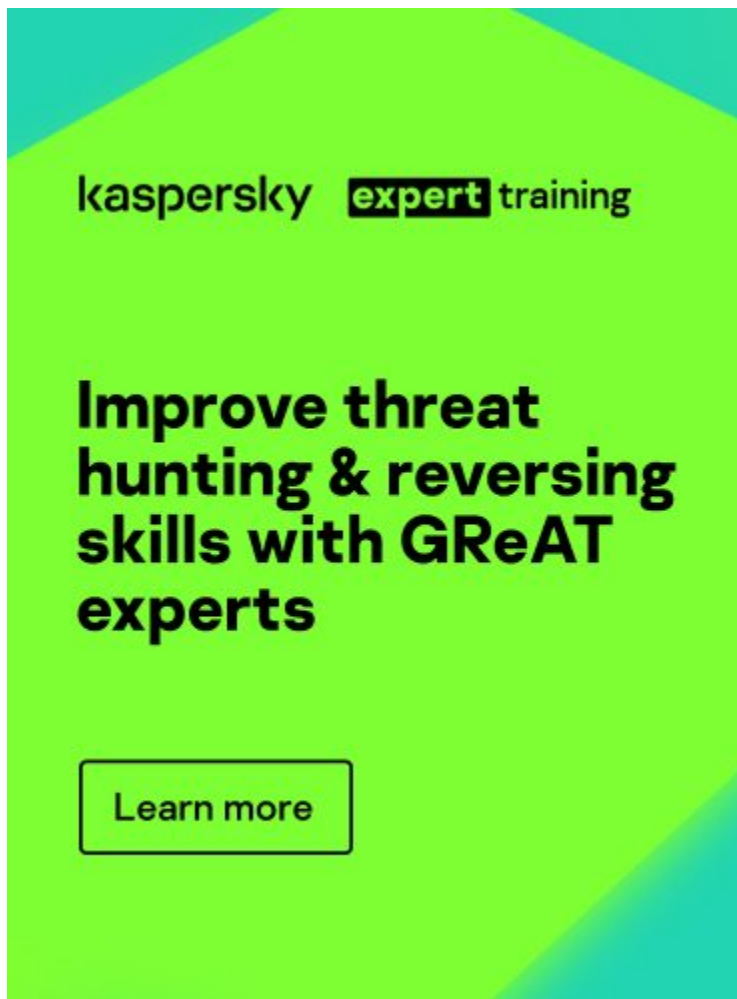
We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

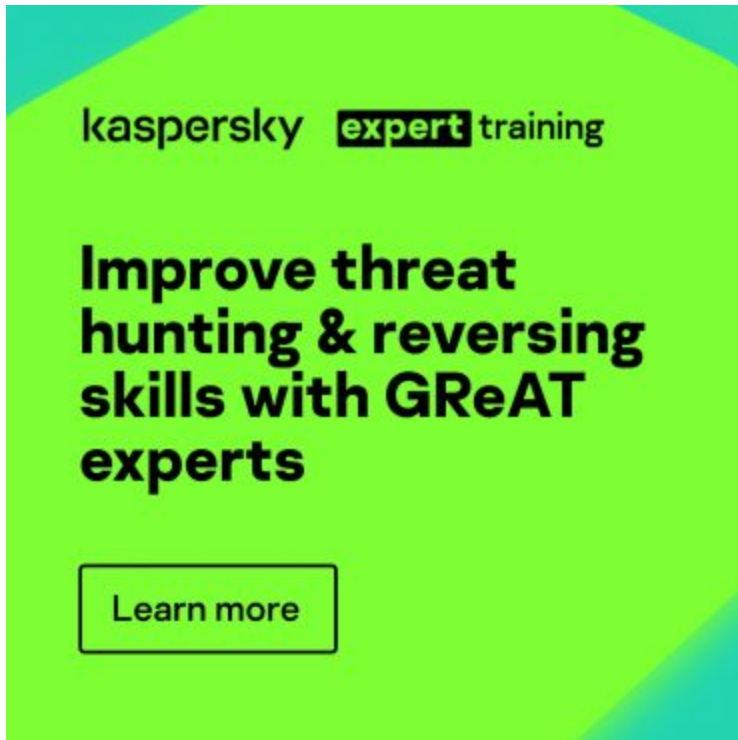
It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

A promotional graphic for Kaspersky Expert Training. The background is a vibrant green with teal triangular accents in the corners. At the top left, the text 'kaspersky expert training' is displayed, with 'expert' in a black box. The main headline reads 'Improve threat hunting & reversing skills with GReAT experts' in large, bold, black font. At the bottom, there is a white rectangular button with a black border containing the text 'Learn more'.

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-

A promotional banner for Kaspersky Expert Training. The background is a vibrant lime green with teal triangular accents in the corners. The text is in a clean, sans-serif font. At the top left, it says 'kaspersky expert training' where 'expert' is in a black box. Below that, the main headline reads 'Improve threat hunting & reversing skills with GReAT experts'. At the bottom left, there is a white rectangular button with a black border containing the text 'Learn more'.

kaspersky **expert** training

**Improve threat
hunting & reversing
skills with GReAT
experts**

Learn more