Urgent Call for Companies to Patch Log4j Vulnerability

17 December 2021

What Happened?

Discovery of Zero Day vulnerability "Log4Shell" in commonly-used Apache Java Package 'Log4j'

- On 9 December 2021, a **critical** vulnerability (CVE-2021-44228 a.k.a. "Log4Shell") impacting multiple versions of the Apache "Log4j 2" was publicly disclosed.
    - The vulnerability can allow unauthenticated **remote code execution** (RCE) and result in **complete takeover** of the affected server.
    - Proof of concept (POC) exploitation tools made available by researchers on the same day.
    - Researchers have noticed cybercriminals already beginning to leverage on the Log4Shell vulnerability.

Where and What is Log4j used for?

An ubiquitous tool in Java-based applications and programmes

- Log4j is an open-source Java logging library developed by the Apache Foundation. It is widely used in many applications and integrated in many services by developers.
    - Any Java application and Java-based product that uses Log4j may be affected.
    - Vulnerable software likely number in the hundreds of thousands, if not millions.
    - Known affected applications/products/services include - Amazon, Cloudflare, Google, Apple iCloud, VMWare Horizon and vCenter Server, Cisco WebEx Server, IBM Qradar, WebSphere, Siemens, and ABB

What is the Impact?

Likely to be massive and widespread; race against time to contain potentially widespread exploitation

- Assigned the Common Vulnerability Scoring System (CVSS) a **maximum severity rating of 10**, based on the **pervasiveness** of the tool, the **ease of exploitation** (even amateur hackers can attack), and the ability to allow attackers to **seize full control** of targeted servers, making it highly attractive to both cybercriminals and nation-state threat actors.
- Such libraries are foundation pieces that are incorporated into a wide range of applications and services and therefore, a single vulnerability in them will have broad implications.
- While fixing of the vulnerability is ongoing, there are already reports of fast-moving actors carrying out large scale efforts to gain footholds in vulnerable networks. To make things worse, disclosure occurred during the **year-end holiday season, fewer resources may be available or activated to remediate**, which does not bode well for such a high severity vulnerability.
    - Exploiting of vulnerability may result in incidents such as coin mining, data theft, ransomware deployment
- Patching it is a **race against time**. Affected products include two broad categories:
    - Products/services supplied by vendors – organisations may face lack of visibility of the components of the software and are dependent on vendors for the fix.
    - In-house developed applications/services – organisations have to assess the status and if their networks are exposed, which services and software need to be fixed, and apply related patches.

What do businesses need to do? (1 of 2)

SingCERT Advisory: Immediate Actions to Protect Against Exploitation of the Apache Java Logging Library Log4j Vulnerability published on 14 Dec 2021

Users (e.g. enterprises and other users who are using products with Log4j)

- If you know you are using it, patch to the latest updates immediately (Java 8: 2.16.0; Java 7: 2.12.2)
    - Proiritise patching starting with mission critical systems, internet-facing systems, and networked servers, and then other IT and OT assets
- Perform a file system search to determine if Log4j is installed in other instances within your System
- The Log4j library is frequently used in software. Check if you are using vulnerable products that uses Log4j (links provided in the SingCERT advisory)
- Deploy protective network monitoring and review system logs
    - Apply Web Application Firewall rules to restrict outbound traffic to known exploit servers
    - Look out for alien Java .class files
    - Check on possible indicators of compromise, e.g. outgoing LDAP connections to Internet destinations before 1 Dec 2021
- If upgrading to the latest version is not possible, apply temporary mitigations

What do businesses need to do? (2 of 2)

SingCERT Advisory: Immediate Actions to Protect Against Exploitation of the Apache Java Logging Library Log4j Vulnerability published on 14 Dec 2021

Vendor (i.e. product developers)

- Identify, mitigate and develop patches that utilise Log4j
- Inform end users of your products that contains this vulnerability and urge them to prioritse software updates

Call for Action

- Businesses need to:
  - Know and understand that the vulnerability is severe
  - Patch or ask your security vendors to patch asap
  - Adopt a heightened security posture (check for unusual network behaviour)
  - Review resources (on the next slide) as part of the measures to enhance your cybersecurity posture

- Report a compromise to SingCERT. This will help alert us to an ongoing attack in SG

https://go.gov.sg/singcert-incident-reporting-form

(Incident Category: Malware/Device-related

Incident Type: Others)

- Contact your security vendor or engage a cybersecurity vendor for immediate incident response

Resources

- **Log4j:**

SingCERT Advisory: Immediate Actions to Protect Against Exploitation of the Apache Java Logging Library Log4j Vulnerability published on 14 Dec 2021

https://www.csa.gov.sg/singcert/Advisories/ad-2021-010

- **Toolkits:**

Cybersecurity Toolkit for Enterprise Leaders and Cybersecurity Toolkit for SME Owners

https://www.csa.gov.sg/Programmes/sgcybersafe/cybersecurity-toolkits/leaders

Incident Response Checklist

https://www.csa.gov.sg/gosafeonline/-/media/Gso/Files/Resources/CSA-Incident-Response-Checklist.pdf

Protect your Systems and Data from Ransomware Attacks

https://www.csa.gov.sg/singcert/Advisories/ad-2020-006

Thank you