PO Box 10189
Grand Cayman KY1-1102
Cayman Islands
Tel: (345) 946-4282

UTILITY REGULATION AND COMPETITION OFFICE

23 December 221

Apache Log4J Java logging library - vulnerability notice

OfReg is issuing a notice advising organisations to note and take appropriate steps to mitigate any potential impact of vulnerabilities affecting applications using the Apache Log4j Java logging library.

Apache Log4j is part of the Apache Logging Services project of the Apache Software Foundation, widely used in many applications and is present in many services as a dependency. This includes enterprise applications, including custom applications developed within an organization, as well as numerous cloud services.

The Global Cyber Security Community has classified this vulnerability as CRITICAL.

This could allow for arbitrary code execution which can be executed remotely. In most cases, developers may write error messages caused by user input into the log. Attackers can use this feature to construct special data request packets through this vulnerability and ultimately trigger remote code execution.

Organisations and their developers are advised to discover where Log4j is installed in their organisations infrastructure and install the latest updates immediately.

Threat intelligence

According to numerous open-source reports, Log4j is used with Apache software like Apache Struts, Solr, Druid, along with other technologies. Many websites of manufacturers and providers have been found to be affected including Apple, Twitter, Steam, Tesla and more. Threat actors will likely include payloads in simple HTTP connections, either in a User-Agent header or trivial POST form data. In addition, it has been reported that organizations are already seeing signs of exploitation in the wild with further attempts on other websites likely.

What are the vulnerabilities?

There are three vulnerabilities detailed here: https://logging.apache.org/log4j/2.x/security.html?s=09

1. CVE-2021-44228 – CVSS Base 10
2. CVE-2021-45046 – CVSS Base 9
3. CVE-2021-45105 – CVSS Base 7.5

Thousands of commercial and open-source IT products are affected by these vulnerabilities. More information, including lists of affected products, and guidance on how to mitigate the vulnerability and detect exploitation, are available from the US Cybersecurity & Infrastructure Agency (CISA) at https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance.

PO Box 10189
Grand Cayman KY1-1102
Cayman Islands
Tel: (345) 946-4282

UTILITY REGULATION AND COMPETITION OFFICE

Additional resources:

CISA: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

CISA's list of affected software: https://github.com/cisagov/log4j-affected-db

NCSC's list of affected software: https://github.com/NCSC-NL/log4shell/tree/main/software

CIS' flowchart on this advisory: https://www.cisecurity.org/log4j-zero-day-vulnerability-response/

ENDS.

ABOUT OFREG

The Utility Regulation and Competition Office ('OfReg' or the 'Office') is the independent regulator established by section 4 of the Utility Regulation and Competition Act (as revised) (the 'URC Act') for the electricity, information, and communications technology, water, wastewater, and fuel sectors in the Cayman Islands.

OfReg provides the opportunity for consistency and collaboration in regulation across the energy, fuel, ICT, and water sectors; better utilisation of skills and resources resulting in more efficient and effective regulatory processes; encouraging competition where appropriate and feasible; championing sustainability and innovation across markets, contributing to the economic and social goals of the Cayman Islands.

Media Contact
Daniel Lee
Manager - Consumer Affairs & Public Education
Daniel.Lee@ofreg.ky