National Cyber Security Centre

2112101241-NCSC

A part of the **Department of the Environment, Climate & Communications**

NCSC Alert

Critical 0-day vulnerability in Apache Log4j library - CVE-2021-44228
2021-12-10

Status: TLP-WHITE

This document is classified using Traffic Light Protocol. Recipients may share TLP-WHITE *information freely, without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.*

Description

A serious vulnerability has been identified and fixed in Apache Log4j, an open source java logging library used by many web applications and services (CVE-2021-44228).

The vulnerability allows an unauthenticated remote attacker to execute arbitrary code with the privileges of the web server. The 0-day that can be exploited by logging a crafted string. Java Naming and Directory Interface (JNDI) triggers a look-up on a server controlled by the attacker and executes the returned code. A proof of concept (PoC) has been published on GitHub. It is likely that malicious actors will shortly begin using this vulnerability to attack webservers. The NCSC advises that organisations assess their web servers for exposure to this risk. This should include services administrated and provided by third party service providers.

Apache has published a update and administrators should conduct their patch process to update to log4j-2.15.0-rc2.

Attempts to exploit the vulnerability can be detected as log files for any services using affected log4j versions will contain user-controlled strings, for example, “Jndi:ldap”. Independent researchers have published tools to help identify attempts to exploit this vulnerability.

Products Affected

Version of Apache log4j prior to log4j-2.15.0-rc2.
Many services use the logging library and are vulnerable to full server compromise. These can include cloud service and services like Apache Struts.

Impact

Remote Code Execution - compromised systems.

Mitigations

The NCSC advises that updates be applied to vulnerable systems in accordance with local change management process.

If immediate patching is not possible, administrators of vulnerable systems can start the server with the *JVM option -Dlog4j2.formatMsgNoLookups = true* as a temporary mitigation measure.

Recommendations

The NCSC recommends that all organisations update to the latest version of Apache log4j and apply the mitigation measure if immediate update is not possible, in line with local change management process. Organisations should examine logs for attempts to exploit the vulnerability and establish alerts if attempts are made post update.

Organisations should confirm with their service providers that mitigation measures against this vulnerability are in place.

DISCLAIMER: *This document is provided "as is" without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.*

National Cyber Security Centre
29-31 Adelaide Road,
Dublin, D02 X285,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@decc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie