Log4j CRITICAL Vulnerability - CVE-2021-44228

Here we have collected information which may be useful to sites, Federated cloud users, and others.

We have NOT so far identified any EGI services as being exposed to this vulnerability.

General information

A flaw was found in the Java logging library Apache Log4j 2 which could allow a remote attacker to execute code on the server if the system logs an attacker controlled string value, as reported by

https://www.lunasec.io/docs/blog/log4j-zero-day/

Note that this is true for clients using log4j as well as services.

It should be noted that this vulnerability is fixed in 2.16 The fix in 2.15 was incomplete

****UPDATED on 6th January 2022****

The update in 2.16 was incomplete, those running Java 8 should update to Log4j 2.17.1.

Those running Java 7 should update to 2.12.4, Those running Java 6 should update to 2.3.2.

See the Log4j website at:

Log4j – Apache Log4j Security Vulnerabilities

Some advisories from different providers are collected here:

https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

Some affected software is collected here:

https://github.com/NCSC-NL/log4shell/tree/main/software

https://github.com/YfryTchsGD/Log4jAttackSurface

You can find additional information at the pages and in the heads up documented below.

https://www.govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

https://github.com/NorthwaveSecurity/log4jcheck

Temporary Mitigation

Limited and temporary mitigation might be available, see:--

https://www.lunasec.io/docs/blog/log4j-zero-day/#temporary-mitigation

https://access.redhat.com/security/cve/CVE-2021-44228

Please ensure **at least** that any potentially affected service is **not exposed** to the **internet !**

For EGI Services

Sites and those providing EGI services should be reminded that if anyone becomes aware of any site or service where this (or any other vulnerability) has been exploited, the EGI CSIRT must be informed according to the procedure at

SEC01 EGI CSIRT Security Incident Handling Procedure