CYBER DEFENSE AFRICA: SECURITY ANNOUNCEMENT **Date**: 12/12/2021

Type of Content	Description
Title	*Zero-day in the Log4j Java library*
Id	*202112/Alert/01*
Code LTP	*White*
Risk Level	*High*
Application and service Assigneds	*Druide Apache*, Apache *Flinkn*, Apache *Solr*, Apache *Spark*, Apache *Struts2 , Apache Tomcat*
Version	*2.0 and 2.14.1*
Platform	*Apache Struts*
Update	*Log4j-2.15.0-rc2*
Summary	*Vulnerability that allows unauthenticated remote code execution and access to servers.*
Impacts	*Totalaccess to affected servers*
Detailed description	*The Apache log4j library allows developers to log various data within their application. In some circumstances, the recorded data comes from user input. If this user entry contains special characters and is then saved in the context of log4j, the Java method lookup will eventually be called to execute the remote user-defined Java class on the LDAP server. This will in turn lead to RCE on the victim server that uses the vulnerable log4j 2 instance.*
Solutions	*It is requested to make an update Log4j-2.15.0-rc2.* *With the release of the official Apache patch, it was initially reported that 2.15.0-rc1 had patched CVE-2021-44228. However, a later bypass was discovered. A new version 2.15.0-rc2 has been released in turn, which protects users from this vulnerability.* *Note: Log4j 2.15.0 requires Java 8. Therefore, organizations using Java 7 will need to upgrade before they can upgrade to the patched version of Log4j.*
Links for more details	*https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability*