Log4j Vulnerability Analysis in Enable-U Products (CVE-2021-44228)

Products		Version	State	Note
Enable-U Products	OpenTunnel	from 2.0.0	Not affected	Opentunnel does not include log4j. Opentunnel is using the logging infrastructure of jboss 6/wildfy. JBoss Logmanager is not using log4j either.
	CloudConnector	from 1.0	Not affected	log4j v. 1.2.17 is used
	EventBroker	1.7.0	Not affected	See https://enableu.atlassian.net/browse/EVENTBROKE-741
	StelselPlus	1.8.0, 2.0.0	Not affected	See https://enableu.atlassian.net/browse/RSGB-870

	CFS	1.2.0	Not affected	Used logging APIs:
				`commons-logging`
				`org.slf4j:slf4j-api`
				`org.jboss.logmanager:jboss-logmanager`
				`org.jboss.logmanager:jboss-logmanager-log4j`
				Uses logging infrastructure of WildFly 12.

	LVWOZ TT	2.0.3	Not affected	Uses logging infrastructure of WildFly
	STP	3.2.0	Not affected	Uses logging infrastructure of WildFly

	BB Portal	4.0.1	Not affected	Used logging APIs:
				`commons-logging`
				`org.slf4j:slf4j-api`
				`org.jboss.logmanager:jboss-logmanager`
				`org.jboss.logmanager:jboss-logmanager-log4j`
				Uses logging infrastructure of WildFly 12.

	BB Broker	from 1.0.0	Not affected	Uses logging infrastructure of WildFly
Open Source Software used in Enable-U Products	JBoss AS 6	All versions	Not affected	Logging is handled by JBoss Logmanager which is not using log4j.
	Wildfly	All versions	Not affected	Logging is handled by JBoss Logmanager which is not using log4j.
	Keycloak	3.4.3, 11.0.3, 12.0.4	Not affected	Keycloak includes only the Log4j API in the server distribution. Logging is handled by JBoss Logmanager, not Log4j directly according to Keycloak devs: https://github.com/keycloak/keycloak/discussions/9078