Log4J Vulnerabilities - Thales Resolutions (Updated to 20 Dec 2021)

The information provided below is referred from https://supportportal.thalesgroup.com/csm?id=kb_article_protected&sys_id=021d8257db980110520c4705059619be and https://supportportal.gemalto.com/csm?id=kb_article_view&sys_kb_id=12acaed3dbd841105d310573f3961953&sysparm_article=KB0025297.

- **CVE Number**

  2021-44228

- **Discovery Date**

  No Information

- **Threat Level**

Critical

- **Response to Log4j**

On December 10, Thales Cloud Protection and Licensing was made aware of a zero-day exploit in the popular Java logging library Log4J, impacting versions 2.14.1 and lower. An attacker who can control log messages or log message parameters to an affected system, has the ability to execute arbitrary code loaded from an attacker controlled internet server. Full details can be found in the public advisory (CVE-2021-44228).

Further to our initial posting, a new advisory (CVE-2021-45046) has been released detailing that in some instances the remediation from CVE-2021-44228 was insufficient. As of December 15, 2021 this bulletin also reflects the status of this CVE as well.

- **Affected Thales Products**

Thales has taken immediate action to investigate the impact of this vulnerability to our products and services.

1. CADP/SafeNet Protect App (PA) – JCE
2. CipherTrust Batch Data Transformation (BDT) 2.3
3. CipherTrust Cloud Key Manager (CCKM) Appliance
4. CipherTrust Vaulted Tokenization (CT-V) / SafeNet Tokenization Manager CipherTrust/SafeNet PDBCTL
5. Crypto Command Center (CCC)
6. SafeNet Vaultless Tokenization
7. Sentinel LDK EMS (LDK-EMS)
8. Sentinel LDKaas (LDK-EMS)
9. Sentinel EMS Enterprise aaS
10. Sentinel Professional Services components (both Thales hosted & hosted on-premises by customers)
11. Sentinel SCL

12. Thales Data Platform (TDP)(DDC)

Other Thales products are tested and assumed not to be affected.

- **Thales Mitigation**

Thales CPL has taken action to upgrade systems immediately in accordance with these recommendations and checking logs for signs of compromise. All systems with the above versions have been patched.

Customers using the impacted products on-premises should immediately update the relevant patch according to the Thales official documentation. The Thales official documentation needs to login to the Thales support portal to get it.

The support portal link:

https://supportportal.thalesgroup.com/csm?id=kb_article_protected&sys_id=021d8257db980110520c4705059619be

Thales Software Monetization recommends organizations running Apache Log4j take the following actions:

Check for vulnerable versions of Apache Log4j in your environments and applications.
Implement latest patch to production environments as soon as possible. Monitor for security bulletins.
Monitor for vendor patches as they become available.