8840 Stanford Blvd.
Suite 2100
Columbia, MD 21045
410.290.1411
owlcyberdefense.com

Product Advisory

Date: December 16, 2021

From: Owl Cyber Defense

Subject: Owl Commercial Product Lines and Log4j Vulnerabilities (CVE-2021-44228)

Importance: High

Operational Impact: Low

Advisory Description: A vulnerability (CVE-2021-44228) in the Apache Log4j package has been identified. The vulnerability has been rated at the highest level of severity in the CVE system.

Owl Cyber Defense Solutions has reviewed all commercial product lines and determined that that Log4j is not used in any products. No Owl commercial product has the CVE-2021-44228 vulnerability.

In addition, Owl's data diode technology prevents exploitation of this vulnerability in equipment protected by our products. Because this vulnerability relies on a callback feature in Log4j, blocking all return traffic is an effective protection mechanism. *For these reasons, Owl has rated the Operational Impact as "Low".*

Affected Products: DiOTa, EPDS, IXD, OCCS Card Kits, OPDS-5D, OPDS-100D, OPDS-100, OPDS-1000, OPDS-MP, PaciT, ReCon, SSUS, XD Matrix and other variants.

Course of Action: No action needed.