KEMENTERIAN PENDIDIKAN TINGGI, SAINS, DAN TEKNOLOGI
UNIVERSITAS LAMPUNG
CSIRT — COMPUTER SECURITY INCIDENT RESPONSE TEAM
Jalan Prof. Dr. Sumantri Brojonegoro No. 1, Bandar Lampung 35145
Laman: csirt.unila.ac.id · Surel: csirt@unila.ac.id · Telepon: (0721) xxx-xxxx

Nomor : ADV/CVE-2021-44228/2026
Perihal : Dokumen Hasil Analisis AI CSIRT

SECURITY ADVISORY — PERINGATAN KERENTANAN KRITIS APACHE LOG4J

Tingkat Keparahan: CRITICAL CVE: CVE-2021-44228 CVSS: 10.0
Dipublikasikan: 22 Jun 2026 Sumber: BSSN / NVD

Ringkasan:
Kerentanan Remote Code Execution pada Apache Log4j2 (Log4Shell) memungkinkan penyerang mengeksekusi kode arbitrer melalui input yang dicatat ke log. Banyak aplikasi Java di lingkungan kampus berpotensi terdampak. Eksploitasi aktif terpantau di internet.

Sistem yang Terpengaruh:
- Apache Log4j 2.0-beta9 hingga 2.14.1
- Aplikasi Java yang menggunakan Log4j2 untuk logging
- Layanan internal berbasis Spring Boot / Elasticsearch lama

Langkah Mitigasi yang Disarankan:
1. Perbarui Log4j ke versi 2.17.1 atau lebih baru.
2. Jika tidak bisa update, set log4j2.formatMsgNoLookups=true.
3. Hapus kelas JndiLookup dari classpath.
4. Batasi koneksi keluar (egress) dari server aplikasi.
5. Pantau log untuk pola ${jndi:ldap://...}.

Indikator Kompromi (IOC):
- Pola String: ${jndi:ldap://
- IP: 45.155.205.233
- File Hash (SHA256): a1b2c3...d4e5 (contoh payload .class)
- URL: hxxp://malicious-ldap[.]example/exp

Tindakan Prioritas:
Identifikasi seluruh aset yang menggunakan Log4j dalam 24 jam dan lakukan patching prioritas pada layanan yang terekspos ke internet.

Bandar Lampung, 12 September 2026
Ketua CSIRT Universitas Lampung

(.....)
Tanda tangan elektronik (TTE/BSrE) menyusul.