# CVE Report

**CVE ID:** CVE-2021-44228  
  
**Summary:** Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.  
  
**Base Score:** 10.0 CRITICAL  
  
**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H  
  
**Reference:** http://packetstormsecurity.com/files/165225/Apache-Log4j2-2.14.1-Remote-Code-Execution.html

**Affected Systems Information:** Cisco » Emergency Responder Versions before (<) 11.5\(4\)  
cpe:2.3:a:cisco:emergency\_responder:\*:\*:\*:\*:\*:\*:\*:\*  
Matching versions

**Exploit Links to Download:**  
  
https://www.exploit-db.com/download/51183  
https://www.exploit-db.com/download/50590  
https://www.exploit-db.com/download/50592  
  
  
**Exploit Links to Look:**  
  
https://www.exploit-db.com/exploits/51183  
https://www.exploit-db.com/exploits/50590  
https://www.exploit-db.com/exploits/50592