Patches of dangerous vulnerabilities being exploited by hackers contain dangerous holes and then continue to be exploited by hackers

Not long after the Log4j vulnerability was discovered, the patch was released. However, the irony is that this patch has holes.

In early December, the world was shocked when a critical code execution vulnerability was discovered in Log4j, a utility used by virtually every cloud computing service and enterprise network. Immediately, open source developers released an update to patch the bug and urged users to install the patch immediately.

Now researchers report that there are at least two vulnerabilities in the Log4j 2.15.0 patch update. Not only that, hackers are also exploiting one of those two vulnerabilities, targeting targets that have installed the patch. Therefore, the researchers once again urge everyone to quickly install the Log4j 2.16.0 update to patch the vulnerability being tracked under the code CVE-2021-45046.

According to the researchers, patch 2.15.0 is incomplete in some non-default configurations, creating an opportunity for hackers to perform DDoS attacks. This can cause the attacked servers to be completely paralyzed until restarting or other actions are taken.

Version 2.16.0 fixes this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

The remaining vulnerability in patch 2.15.0 discovered by security firm Praetorian is related to information leakage. Hackers can exploit this vulnerability to download data from affected servers. The company has reported the issue to the Apache Foundation but still strongly advises users to install patch 2.16.0 as soon as possible.