

Vulnerability Overview

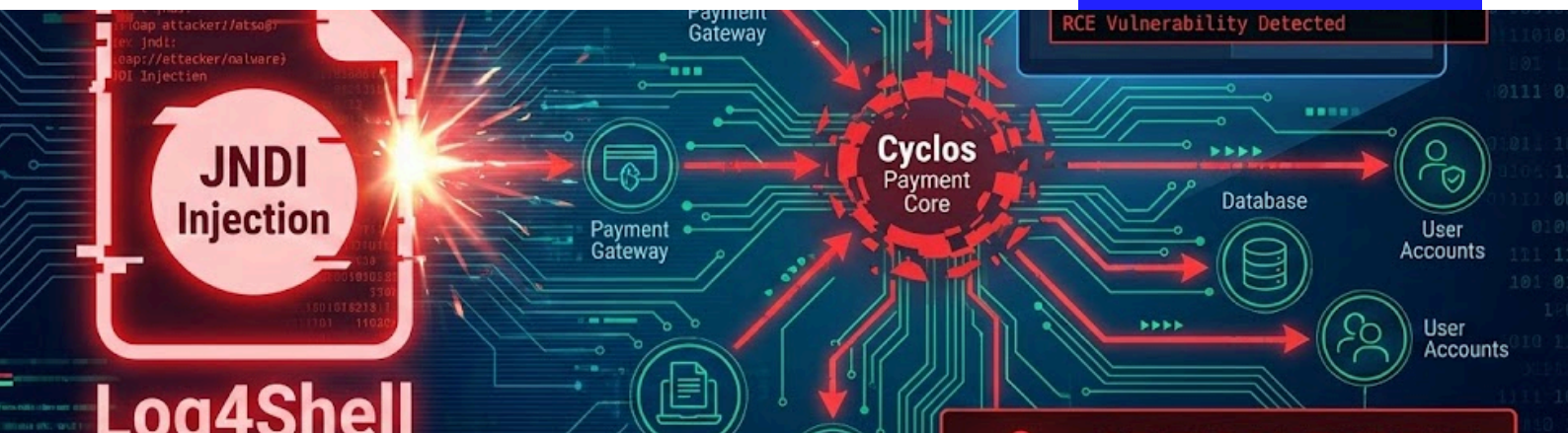
Cyclos Payment System

Remote Code Execution (CVE-2021-44832)

Vulnerability Rating

Critical

CVSS v3 10.0



Introduction

Cyclos is a payment software platform used by banks, barter systems, remittance providers, and other monetary-innovation programs, reportedly used by 1,500+ payment systems worldwide. CyStack assessed that Cyclos versions prior to 4.14.15 can be exposed to remote code execution (RCE) due to inclusion of a vulnerable Log4j library.

Synopsis

In the technical analysis, we attribute the root cause to Log4j "Log4Shell" behavior, noting that Log4j 2.14.1 (present in the tested Cyclos build) is vulnerable under CVE-2021-44228 (Log4Shell).

Affected

This vulnerability affected Cyclos Payment System with versions prior to 4.14.15 and was the culprit behind the infamous hack of a cryptocurrency exchange platform name ONUS. The team at CyStack managed to find the vulnerability during an in-depth investigation of the incident that exposed 2 million personal users' information.

Details

Log4j usage confirmation inside the Cyclos codebase (including references in relevant JARs) was present, with identification of a vulnerable entry point where attacker-controlled data can reach logging and trigger JNDI lookups, enabling RCE under the described conditions. Furthermore, there is validation via a controlled demonstration that resulted in arbitrary file write on the server (as evidence of successful exploitation flow).

Timeline of incident

- **December 9, 2021:** Public disclosure of Log4Shell begins broad industry response.
- **December 11-13, 2021:** Exploitation of Log4Shell through Cyclos on ONUS infra, backdoors installed
- **December 14, 2021:** ONUS was notified by Cyclos about the vulnerability, emergency patch deployed
- **December 23, 2021:** Abnormal activities were detected, incident responses deployed
- **December 24, 2021:** Ransom request from the attackers, ONUS disclosure of the attack to users

Learn more

[CyStack Advisories](#)

[NIST Vulnerability Database](#)

[Incident Research](#)

Your **Trusted Security Partner**

CyStack