# Remoting

Language: Deutsch · **English**

## Remoting

> **Security notice about the remoting interface – CVE-2016-1000027, mitigations and the switch to JSON from 4.2023.8.**

KONZEPT | ADMINISTRATOR | UPDATED: JUL 2026 | APPLIES TO NUCLOS 4.2026.X

**On this page**



**Security notice**

In all Nuclos versions **up to 4.2023.7** the remoting interface (used by the rich client) is vulnerable. An update to **4.2023.8** is strongly recommended.

### Cause

Communication with the rich client ran via Java RMI/Spring HttpInvoker over HTTP(S). Via CVE-2016-1000027 Java deserialization allows **remote code execution**: anyone with access to the remoting interface can send crafted requests and run code as a subprocess of the server. All URLs matching `*/remoting/*` are affected.

### Mitigations for versions  4.2023.7

- **Block** the remoting interface in the proxy/web server or allow it only for trusted IP ranges (all `*/remoting/*` URLs).
- From 4.2022.14: restrict IP ranges via `SECURITY_IP_ALLOW_REMOTING` (see security parameters).

### Version 4.2023.8

From this version a fully **JSON**-based remoting interface is available. Java RMI is **disabled** by default but can be re-enabled with `remoting.java-rmi.enabled=true` in `server.properties` (reset by the installer).

### Related pages

**Security parameters**

IP filter.

Open

**Running Nuclos behind a reverse proxy**

Proxy.

Open