Remoting

Sprache: **Deutsch** · English

Remoting

> **Sicherheitshinweis zur Remoting-Schnittstelle – CVE-2016-1000027, Gegenmaßnahmen und die JSON-Umstellung ab 4.2023.8.**

KONZEPT | ADMINISTRATOR | STAND: JUL 2026 | GILT FUER NUCLOS 4.2026.X

Auf dieser Seite

Sicherheitshinweis

In allen Nuclos-Versionen **bis 4.2023.7** ist die Remoting-Schnittstelle (vom Rich Client genutzt) angreifbar. Ein Update auf **4.2023.8** wird dringend empfohlen.

Ursache

Die Kommunikation mit dem Rich Client lief über Java-RMI/Spring HttpInvoker über HTTP(S). Über CVE-2016-1000027 ermöglicht die Java-Deserialisierung eine **Remote Code Execution**: Wer Zugriff auf die Remoting-Schnittstelle hat, kann präparierte Anfragen senden und Code als Unterprozess des Servers ausführen. Betroffen sind alle URLs mit `*/remoting/*`.

Maßnahmen für Versionen 4.2023.7

- Remoting-Schnittstelle im Proxy/Webserver **blocken** oder nur für vertrauenswürdige IP-Bereiche freigeben (alle `*/remoting/*`-URLs).
- Ab 4.2022.14: IP-Bereiche über den Parameter `SECURITY_IP_ALLOW_REMOTING` beschränken (siehe Security-Parameter).

Version 4.2023.8

Ab dieser Version steht eine komplett auf **JSON** umgestellte Remoting-Schnittstelle bereit. Java-RMI ist standardmäßig **deaktiviert**, lässt sich aber per `remoting.java-rmi.enabled=true` in der `server.properties` reaktivieren (wird vom Installer zurückgesetzt).

Verwandte Seiten

Security-Parameter

IP-Filter.

Öffnen

Betrieb von Nuclos hinter einem ReverseProxy

Proxy.

Öffnen