Remoting

Achtung!
In allen Nuclos Versionen bis 4.2023.7 ist die Remoting Schnittstelle, welche vom Rich-Client verwendet wird, angreifbar.
Ursache und Maßnahmen werden nachfolgende erläutert.

Auslöser / Ursache

Durch regelmäßige Abhängigskeits-Scans in unserer Build-Pipeline wurde ein CVE angezeigt, welcher auf mögliche Lücken Hinwies:

https://nvd.nist.gov/vuln/detail/CVE-2016-1000027

Hersteller-Dokumentation der betroffenen Komponente:

https://docs.spring.io/spring-framework/docs/current/reference/html/integration.html#remoting-httpinvoker

In einer weiteren Analyse lässt sich die Ausnutzung auf die Java Serialisierung zurückführen, im spezifischen Fall wird eine Komponente von Spring (HttpInvoker) angreifbar für eine sogenannte **Remote Code Execution**.
Dies bedeutet, mit einer präparierter Anfrage deserialisiert Java/Spring das ankommende Binär-Objekt zu einer Java-Klasse welche wenn selbst verändert Mittels Reflection Java-Programmcode ausführt, der Angreifer kann auf dem entfernten Server jegliches Kommando ausführen als Unterprozess vom Serverprozess.

Möglich wird dies in Nuclos dadurch, dass die Kommunikation mit dem Rich-Client über besagte Schnittstelle (Java RMI - Remote Method Invocation) läuft welche über HTTP/HTTPS zu dem Server transportiert wird.
Jeder der Zugriff auf die Remoting Schnittstelle des Nuclos-Servers hat, kann eine solche präparierte Anfrage an den Server senden.

Da die Kommunikation in beider Richtung über die gleiche Implementation/Schnittstelle läuft, könnte auch ein kompromittierter Server an Richclients schadhaften Code verteilen.

Ziel-Url ist zum Beispiel:
<base-server-url>/<application context e.g nuclos>/remoting/ServerMetaService

Maßnahmen für Versionen <= 4.2023.7

- Sollte Nuclos im Internet erreichbar sein per HTTP auch für den Richclient sollte umgehend im Proxy oder Webserver die Remoting Schnittstelle geblockt werden und/oder nur für einen vertrauenswürdigen IP-Bereich freigegeben werden.
  Dies betrifft alle URLs die */remoting/** enthalten.
- Mit Nuclos Version 4.2022.14 wurde ein neuer System Parameter eingeführt um IP-Bereiche zu definieren die für die Remoting Schnittstelle zugelassen sind.
  Security-Parameter (SECURITY_IP_ALLOW_REMOTING)

Ein Update auf **Nuclos 4.2023.8** wird dringend empfohlen!

Version 4.2023.8

Mit dieser Version steht erstmalig eine komplett auf das JSON Format umgestellte Remoting Schnittstelle zur Verfügung. Java RMI wird zusätzlich standardmäßig deaktiviert, kann aber mittels des Eintrages `remoting.java-rmi.enabled=true` in der **server.properties** wieder aktiviert werden.
Achtung, wird vom Installer wieder zurückgesetzt!

Weitere Informationen zur Umstellung finden Sie im Ticket

NUCLOS-9738 - Das Jira-Projekt existiert nicht oder Sie sind nicht anzeigeberechtigt.