Elasticsearch-Server

Elasticsearch[1] ist ein populärer Open-Source-Such-Server auf Basis von Apache Lucene, welcher üblicherweise auf Port 9200/tcp läuft.

Der Elasticsearch-Server selbst unterstützt keine Authentifizierung, wodurch Angreifer nach Belieben die auf dem Server gespeicherten Daten auslesen oder modifizieren können, falls der Server aus dem Internet erreichbar ist. Weiterhin können Angreifer DoS-Angriffe gegen den Server durchführen und (bis zur Version 1.2.x) beliebigen Programmcode auf diesem ausführen.

Im Rahmen des Shadowserver "Open Elasticsearch Server Scanning Projects" werden Elasticsearch-Server identifiziert, welche offen aus dem Internet erreichbar sind. CERT-Bund erhält von Shadowserver die Testergebnisse für IP-Adressen in Deutschland, um betroffene Server-Betreiber benachrichtigen zu können. Weitere Informationen zu den von Shadowserver durchgeführten Tests finden Sie unter [2].

Nachfolgend senden wir Ihnen eine Liste betroffener Systeme in Ihrem Netzbereich. Der Zeitstempel (Zeitzone UTC) gibt an, wann das System geprüft und ein offener Elasticsearch-Server identifiziert wurde. Wir möchten Sie bitten, den Sachverhalt zu prüfen und Maßnahmen zur Absicherung der Elasticsearch-Server auf den betroffenen Systemen zu ergreifen bzw. Ihre Kunden entsprechend zu informieren. Weitere Informationen zur Absicherung eines Elasticsearch-Servers finden Sie unter [3].

Falls Sie kürzlich bereits Gegenmaßnahmen getroffen haben und diese Benachrichtigung erneut erhalten, beachten Sie bitten den angegebenen Zeitstempel. Wurde die Gegenmaßnahme erfolgreich umgesetzt, sollten Sie keine Benachrichtigung mit einem Zeitstempel nach der Umsetzung mehr erhalten.

Referenzen

[1] Elasticsearch [1]
[2] Shadowserver: Open Elasticsearch Server Scanning Project [2]
[3] Elasticsearch: Scripting and Security [3]

Links

[1] https://www.elastic.co/products/elasticsearch
[2] https://scan.shadowserver.org/elasticsearch/
[3] https://www.elastic.co/blog/scripting-security

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/elasticsearch-server/