

# Task: CPE-basiert Richtlinien prüfen

## Inhalt

- CPE-basiert einfache Sicherheitsrichtlinien prüfen
- Problematische Produkte auffinden
- Abwesenheit wichtiger Produkte feststellen

## Einleitung

CPE steht für Common Product Enumeration. Es handelt sich um ein strukturiertes Benennungsschema für IT-Systeme, IT-Plattformen und Softwarepakete.

Mit anderen Worten: CPE bietet eine eindeutige Identifikationsnummer für praktisch jedes Softwareprodukt für das eine Schwachstelle bekannt ist.

Das CPE-Verzeichnis wird von MITRE und NIST gepflegt. MITRE pflegt ebenfalls CVE (Common Vulnerability Enumeration) und andere relevante Sicherheits-Standards.

## Common Product Enumeration (CPE): Name Structure

A CPE Name is a URI with each name starting with the prefix (the URI scheme name) "cpe:".

`cpe:/{part}:{vendor}:{product}:{version}:{update}:{edition}:{language}`

### Part

Each platform can be broken down into three distinct parts. A CPE Name specifies a single part and is used to identify any platform that matches the description of that part. The three distinct parts are:

h = hardware  
o = operating system  
a = application

### Vendor

The second component of a CPE Name is the supplier or vendor of the platform element. For CPE, the name used for a supplier should be the highest organization-specific label of the organization's DNS name.

### Additional Components

The last five components represent product, version, update, edition, and language information. These components are optional. A CPE can be written at different levels of specificity. A name can define product in general, a specific version of a product, or even a certain edition of that product.

### Examples

```
cpe:/o:redhat:enterprise_linux:5  
cpe:/a:sun:jre:1.6.0  
cpe:/a:microsoft:ie:7  
cpe:/a:apache:tomcat:5.5.29
```

Greenbone Networks GmbH, [www.greenbone.net](http://www.greenbone.net)  
Based on CPE documentation (<http://cpe.mitre.org>)

Status 20100208

## CPE-basiert einfache Sicherheitsrichtlinien prüfen

Bei jedem Scan-Vorgang werden die CPEs zu den vorgefundenen Produkten erfasst. Dies passiert unabhängig von der Frage ob die Produkte ein Sicherheitsproblem aufweisen oder nicht.

Auf dieser Basis ist es möglich einfache Sicherheitsrichtlinien zu formulieren und deren Einhaltung zu prüfen.

Mit dem Greenbone Security Manager lassen sich sowohl Richtlinien auf das Vorhandensein von Produkten als auch auf das Fehlen von Produkten formulieren. Diesen Fällen kann jeweils ein Schweregrad zugeordnet werden der dann entsprechend im Bericht auftauchen wird.

## Problematische Produkte auffinden

Dieses Beispiel zeigt wie das Vorhandensein eines bestimmten Produktes in einer IT-Umgebung als schwerwiegendes Problem eingestuft und entsprechend berichtet wird.

1. Die Information ob ein bestimmtes Produkt auf den Zielsystemen vorliegt wird durch ein spezielles oder auch unabhängig voneinander von verschiedenen Network Vulnerability Tests (NVTs)

eingeholt.

D.h., dass man für ein bestimmtes Produkt eine spezifische Scan Configuration erstellen kann die sich ausschließlich auf diese Produkt konzentriert und keine anderen Scans ausführt.






Der Vorteil einer solchen speziellen Scan Configuration ist, dass sie wesentlich schneller ausgeführt werden kann als eine umfangreiche Scan Configuration wie z.B. "Full and Fast".


Der Nachteil einer speziellen Scan Configuration ist, dass man eine gewisse Erfahrung mitbringen sollte um genau die richtigen NVTs auszuwählen und dabei auch eine maximale Trefferwahrscheinlichkeit zu erreichen.

Für den Anfang ist es einfacher, eine umfangreiche Scan Configuration als Basis zu verwenden. Dann braucht man sich nicht um das zu suchende Produkt im besonderen zu kümmern sondern trägt nur dessen CPE entsprechend ein.

Dieses Beispiel geht den einfachen Weg. Als erstes wird eine Kopie der Scan Configuration "Full and Fast" erstellt, denn "Full and Fast" ist als voreingestellte Scan Configuration nicht änderbar.

2. Bearbeiten Sie die eben erstellte Scan Configuration indem sie auf  klicken.

Name	Families		NVTs		Actions
	Total	Trend	Total	Trend	
CPE-based compliance	43		16122		  

3. Auf der Übersichtsseite zu dieser Scan Configuration werden im Abschnitt "Network Vulnerability Test Preferences" alle NVTs die man Parametrisieren kann aufgelistet. Über  kann direkt zur Bearbeitung eines bestimmten NVTs gesprungen werden anstatt sich durch die Familienstruktur durchzuklicken.


CPE-based Policy Check	Single CPE	cpe:/	 
CPE-based Policy Check	CPE List		 
CPE-based Policy Check	Severity	High	 
CPE-based Policy Check	Severity upon	present	 

4. Es läßt sich entweder eine einzelne CPE (in diesem Beispiel wird Internet Explorer 7 angegeben) direkt angeben oder mit Semikolon getrennt eine Liste von CPEs.

In diesem Beispiel wird eingestellt, dass der Schweregrad "High" ausgelöst wird sofern die CPE vorgefunden wird ("present").

Bestätigen Sie Ihre eingaben mit "Save Config".

### Preferences

Name	Value	Actions
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/> <input type="text"/>	
Single CPE	<input type="text" value="cpe:/a:microsoft:ie:7"/>	
CPE List	<input type="text"/> 	
Severity	<input checked="" type="radio"/> High <input type="radio"/> Medium <input type="radio"/> Low	
Severity upon	<input checked="" type="radio"/> present <input type="radio"/> missing	

5. Falls die Erkennungsleistung über lokale Sicherheitstests erhöht werden soll, dann sollte zunächst ein entsprechender Zugang konfiguriert werden. Falls noch nicht geschehen, erstellen Sie dafür einen entsprechenden Anwender auf den Zielsystemen (ein niedrig privilegiertes Benutzer-Konto reicht aus).

### New Credential for Local Security Checks ?

Name

Login

Comment (optional)

Autogenerate credential  
 Password

6. Nun werden die Zielsysteme (Targets) festgelegt und ggf. mit den entsprechenden Credentials verknüpft.

### New Target ?

Name

Comment (optional)

Hosts

Credential (optional)

7. Als nächstes wird die Aufgabe (Task) erstellt. Dafür kombinieren Sie die oben erstellte Scan Configuration mit den erstellten Zielsystemen.



### New Task ?

Name

Scan Config

Scan Targets

Escalator (optional)

8. Der Scan wird gestartet in dem für den eben erstellten Task auf  geklickt wird. Es kann einige Zeit dauern, bis der Scan abgeschlossen ist. Den aktuellen Stand des Scans erhalten Sie indem Sie auf  klicken.

Reports for "CPE-based compliance Task" ?

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Wed Feb 3 16:24:50 2010 Done	High	75	28	54	13	PDF Download	Search X

9. Sobald der Status auf "Done" wechselt, ist der vollständige Bericht verfügbar. Sie können aber auch schon während des Scans die bereits gefundenen Ergebnisse einsehen.

Um sich nur die Ergebnisse der Prüfung der CPE-basierten Sicherheitsrichtlinie anzeigen zu lassen, läßt sich ein entsprechender Filter formulieren (Suchtext "cpe" und, in diesem Beispiel Bedrohungskategorie "High").

Result Filtering

Results 1 - 1 of 1 This report as: PDF Download

Sorting: port\_ascending | port\_descending | threat\_ascending | threat\_descending

Text phrase:

Threat:  High  Medium  Low  Log

Apply

10. In diesem Beispiel wurde der Internet Explorer 7 auf einem der Zielsysteme gefunden und als schwerwiegendes Problem berichtet.

Filtered Results

Host	High	Medium	Low	Log	Total
<a href="#">192.168.2.6</a>	1	0	0	0	1
<a href="#">192.168.2.9</a>	0	0	0	0	0
Total: 2	1	0	0	0	1

**Port summary for host "192.168.2.6"**

Service (Port)	Threat
general/tcp	High

Security Issues reported for 192.168.2.6

**High** general/tcp  
 NVT: CPE-based Policy Check: (OID: 1.3.6.1.4.1.25623.1.0.100353)

The following CPEs have been detected on the remote Host

Policy-CPE|Detected-CPE  
 cpe:/a:microsoft:ie:7|cpe:/a:microsoft:ie:7

For further information see <http://cpe.mitre.org/>

Risk factor : High

## Abwesenheit wichtiger Produkte feststellen

Dieses Beispiel zeigt wie das Fehlen eines bestimmten Produktes in einer IT-Umgebung als schwerwiegendes Problem eingestuft und entsprechend berichtet wird.

1. Führen Sie die Schritte 1 bis 3 wie bei der oben Beschriebenen Methode zum auffinden problematischer Produkte durch.

Bedenken Sie bei der Wahl eines allgemeinen Scans wie "Full and Fast", dass dann sowohl die reiner Anwesenheit eines Produktes auf der Festplatte als auch dessen Ausführung (besonders z.B. als Dienst) gleich behandelt wird.

D.h., falls Sie ganz sicher sein wollen, dass das gewünschte Produkt auch tatsächlich als Dienst aktiv läuft sollten die Prüfungen die lediglich das Vorhandensein prüfen ausgeschaltet werden. Wenn Sie sich die Arbeit noch nicht machen wollen, können Sie bei ausgelösten Alarm aber auch anhand der einzelnen Testergebnisse nachlesen ob ein Dienst oder nur eine Installation gefunden wurde.

2. Diesmal wird die Konfiguration von "CPE-based Policy Check" so vorgenommen, dass der Schweregrad "High" ausgelöst wird sofern Norton Antivirus auf den Zielsystemen fehlt.

Name	Value	Actions
Timeout	<input checked="" type="radio"/> Apply default timeout <input type="radio"/> <input type="text"/>	
Single CPE	<input type="text" value="cpe:/a:symantec:norton_antivirus"/>	
CPE List	<input type="text"/>	
Severity	<input checked="" type="radio"/> High <input type="radio"/> Medium <input type="radio"/> Low	
Severity upon	<input type="radio"/> present <input checked="" type="radio"/> missing	

3. Soll auch das reine Vorhandensein einer Installation des Produktes berücksichtigt werden, dann kann die die Erkennungsleistung über lokale Sicherheitstests erhöht werden. Konfigurieren Sie in diesem Fall einen entsprechender Zugang. Falls noch nicht geschehen, erstellen Sie dafür einen entsprechenden Anwender auf den Zielsystemen (ein niedrig privilegiertes Benutzer-Konto reicht aus).

In Fällen in denen Sie einen laufenden Netzwerk-Dienst suchen, macht dies in der Regel keinen Sinn sondern erhöht die Anzahl der Fehlalarme ("False Positives").

**New Credential for Local Security Checks** ?

Name:



Login:



Comment (optional):

Autogenerate credential  
 Password:

4. Nun werden die Zielsysteme (Targets) festgelegt und ggf. mit den entsprechenden Credentials verknüpft.

5. Als nächstes wird die Aufgabe (Task) erstellt. Dafür kombinieren Sie die oben erstellte Scan Configuration mit den erstellten Zielsystemen.

6. Der Scan wird gestartet in dem für den eben erstellten Task auf  geklickt wird. Es kann einige Zeit dauern, bis der Scan abgeschlossen ist. Den aktuellen Stand des Scans erhalten Sie indem Sie auf  klicken.

Report	Threat	Scan Results				Download	Actions
		High	Medium	Low	Log		
Thu Feb 4 15:11:02 2010 Done	High	75	28	52	19	PDF <input type="button" value="Download"/>	 

7. Sobald der Status auf "Done" wechselt, ist der vollständige Bericht verfügbar. Sie können aber auch schon während des Scans die bereits gefundenen Ergebnisse einsehen.

Um sich nur die Ergebnisse der Prüfung der CPE-basierten Sicherheitsrichtlinie anzeigen zu lassen, läßt sich ein entsprechender Filter formulieren (Suchtext "cpe" und, in diesem Beispiel Bedrohungskategorie "High").

8. In diesem Beispiel wurde Norton Antivirus auf einem der Zielsysteme nicht gefunden.

**Filtered Results**

Host	High	Medium	Low	Log	Total
<a href="#">192.168.2.6</a>	0	0	0	0	0
<a href="#">192.168.2.9</a>	1	0	0	0	1
Total: 2	1	0	0	0	1

**Port summary for host "192.168.2.6"**

Service (Port)	Threat

Security Issues reported for 192.168.2.6

[Back to summary](#)

**Port summary for host "192.168.2.9"**

Service (Port)	Threat
general/tcp	High

Security Issues reported for 192.168.2.9

<b>High</b>	general/tcp
NVT: CPE-based Policy Check (OID: 1.3.6.1.4.1.25623.1.0.100353)	
The following CPEs are missing on the remote Host	
cpe:/a:symantec:norton_antivirus	
For further information see <a href="http://cpe.mitre.org/">http://cpe.mitre.org/</a>	
Risk factor : High	

[Back to summary](#)