

Handlungsempfehlung Fortigate IPS Signatur für die Log4shell/Log4j Schwachstelle

Überprüfung/Aktivierung der IPS Signatur

Vor Einbindung der entsprechenden IPS Signatur bitte die Versionsnummer der IPS Definitionen überprüfen.

Hierzu entweder über die GUI der Fortigate unter „System -> Fortiguard“ im Punkt „License Information“

<ul style="list-style-type: none"> Firmware & General Updates <ul style="list-style-type: none"> Application Control Signatures Device & OS Identification Internet Service Database Definitions Intrusion Prevention <ul style="list-style-type: none"> IPS Definitions IPS Engine Malicious URLs Botnet IPs Botnet Domains Web Filtering <ul style="list-style-type: none"> Blocked Certificates Security Rating Industrial DB <ul style="list-style-type: none"> Industrial Attack Definitions FortiPAM IoT Detection Service FortiGate Cloud 	<ul style="list-style-type: none"> Licensed (Expiration Date: 2022/05/22) Version 6.00741 Version 1.00127 Version 7.02055 Licensed (Expiration Date: 2022/05/22) Version 19.00217 Version 7.00043 Version 3.00215 Version 7.02055 Version 2.00894 Licensed (Expiration Date: 2022/05/22) Version 1.00351 Licensed (Expiration Date: 2022/05/22) Licensed (Expiration Date: 2022/05/22) Version 6.00741 Pending Licensed (Expiration Date: 2022/05/22) Not Activated 	<ul style="list-style-type: none"> Actions Actions View List View List Activate
--	---	--

Oder alternativ in der CLI durch Eingabe des Befehls „get system fortiguard-service status“

```

FGTEST1 # get system fortiguard-service status
NAME          VERSION LAST UPDATE    METHOD    EXPIRE
AV Engine     6.266 2021-08-24 17:02:00 manual 2022-05-22 23:59:59
Virus Definitions 89.7747 2021-12-14 09:04:48 manual 2022-05-22 23:59:59
Extended set  89.7747 2021-12-14 09:04:48 manual 2022-05-22 23:59:59
AI/Machine Learning Malware Detection Model 2.3701 2021-12-14 09:04:48 manual 2022-05-22 23:59:59
Flow-based Virus Definitions 1.000 2021-03-10 09:16:00 scheduled 2022-05-22 23:59:59
Attack Definitions 19.217 2021-12-14 09:18:20 manual 2022-05-22 23:59:59
Attack Extended Definitions 19.217 2021-12-14 09:18:20 manual 2022-05-22 23:59:59
IPS Malicious URL Database 3.215 2021-12-14 09:04:48 manual 2022-05-22 23:59:59
IPS/FlowAV Engine 7.043 2021-02-24 01:19:10 scheduled 2022-05-22 23:59:59
IPS Config Script 1.009 2019-06-06 14:02:00 manual 2022-05-22 23:59:59
Application Definitions 6.741 2021-04-02 23:30:13 scheduled 2022-05-22 23:59:59
Industrial Attack Definitions 6.741 2015-12-01 02:30:00 manual 2022-05-22 23:59:59
  
```

Die eingesetzte Version muss **höher als Version 19.00215** sein, damit die entsprechende Signatur enthalten ist.

Achtung

Für den Fall, dass die genannte Version 19.00215 ist, muss beim Erstellen des IPS die Action auf „Block“ gestellt werden, da der eingestellte Default Wert „Allow“ war. In späteren Versionen ist dies nicht erforderlich.

Überprüfung vorhandener IPS Sensoren

In der GUI der Fortigate unter „Security Profiles -> Intrusion Prevention“

Sollten bereits Sensoren verwendet werden, gilt es zu überprüfen ob die log4shell Signatur in die entsprechenden Filterkriterien fällt.

Hierzu den entsprechenden Sensor editieren, und anschließend unter „IPS Signatures and Filters“ den oder die Filter editieren.

Add Signatures

Falls im Sensor Filter verwendet werden (Type)

kann durch Suchen nach „51006“ überprüft werden ob die entsprechende Signatur in den Filterkriterien enthalten ist.

Name	Severity	Target	OS	Action	CVE-ID
IPS Signature 1/7529					
Apache.Log4j.Error.Log.Remote.Code.Executi...	■■■■■	Server	All	⊘ Block	CVE-2021-44228

Bleibt die Ausgabe leer, entspricht die Signatur nicht den Filterregeln. Es bedarf entweder Anpassung der Filterregel, oder aber die Signatur muss einzeln dem IPS Sensor hinzugefügt werden (bspw. analog zum Punkt „[Erstellung eines neuen IPS Sensors](#)“).

Für den Fall dass im Sensor einzelne Signaturen verwendet werden ((Type Filter Signature))

Muss die entsprechende Signatur manuell hinzugefügt werden.

Add Signatures

Type: Filter | Signature

Action: Default

Packet logging: Enable | Disable

Status: Enable | Disable | Default

Rate-based settings: Default | Specify

Exempt IPs: 0 | Edit IP Exemptions

Add All Results | 51006 | Selected 0 | All

	Name	Severity	Target	OS	Action	CVE-ID
<input checked="" type="checkbox"/>	Apache.Log4j.Error.Log.Remote.Code.Exec...	■■■■■	Server	All	Block	CVE-2021-44228

Anschließend mit **OK** bestätigen und im Fenster des IPS Sensors, ebenfalls mit **OK** bestätigen

Der IPS Sensor kann jetzt wie unter „[Einbinden des Intrusion Protection Profils in die Firewall Policies](#)“ eingebunden werden

Erstellung eines neuen IPS Sensors

Soll ein IPS Sensor erstellt werden der ausschließlich zur Blockierung der Log4Shell Lücke verwendet wird:

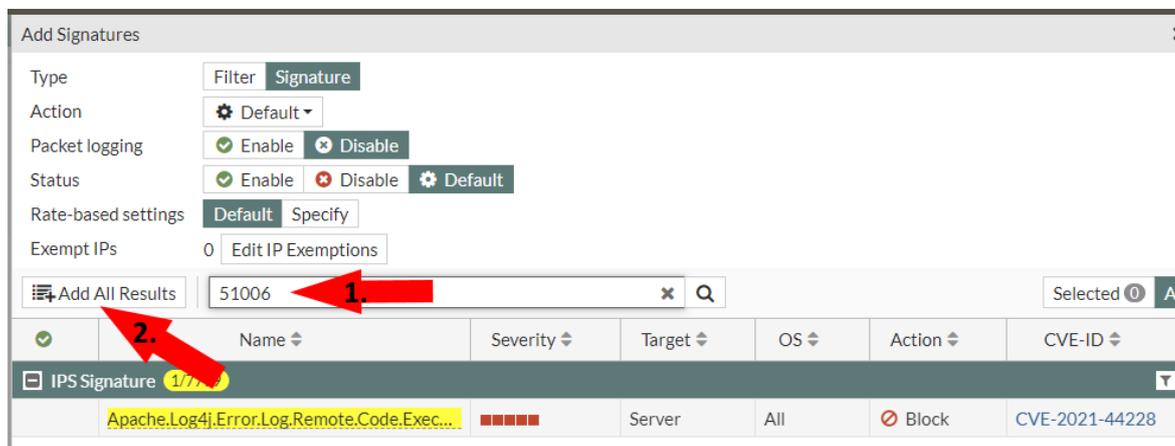
In der GUI der Fortigate unter „Security Profiles -> Intrusion Prevention“

Oben auf „Create New“ und anschließend einen Namen für den IPS Sensor eingeben, bspw. „IPS_log4j“

Im Punkt IPS Signatures and Filters auf „Create New“ und anschließend den Type auf Signature ändern.

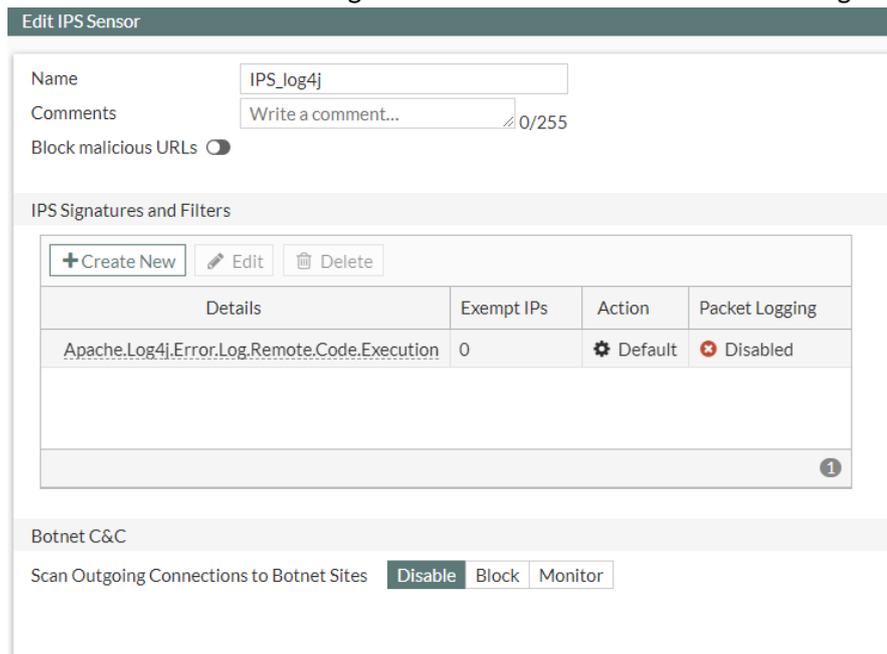
Im Suchfeld nach „51006“ suchen, den Eintrag in der Liste markieren und auf „Add All Results“ klicken.

Die Auswahl wird durch Anzeige  bestätigt.



Name	Severity	Target	OS	Action	CVE-ID
Apache.Log4j.Error.Log.Remote.Code.Exec...	■■■■■	Server	All	Block	CVE-2021-44228

Anschließend mit **OK** bestätigen Der erstellte IPS Sensor sollte wie folgt aussehen



Details	Exempt IPs	Action	Packet Logging
Apache.Log4j.Error.Log.Remote.Code.Execution	0	Default	Disabled

Die Erstellung des IPS Sensors ebenfalls mit **OK** bestätigen.

Einbinden des Intrusion Protections Profils in die Firewall Policies

In der GUI der Fortigate unter „Policy & Objects -> Firewall Policy“ die entsprechenden Policies bearbeiten und das IPS Profil anhängen.

Name ⓘ Log4j Testpolicy

Incoming Interface lan

Outgoing Interface a

Source all

IP/MAC Based Access Control ⓘ

Destination all

Schedule always

Service ALL

Action ACCEPT DENY

Inspection Mode Flow-based Proxy-based

Firewall / Network Options

NAT

Protocol Options PROT default

Security Profiles

Web Filter

Video Filter

IPS IPS IPS_log4j

SSL Inspection

Logging Options

Log Allowed Traffic

Comments

Enable this policy

IPS IPS_log4j

Search + Create

- IPS all_default
- IPS all_default_pass
- IPS default
- IPS high_security
- IPS IPS_log4j
- IPS protect_client
- IPS protect_email_server
- IPS protect_http_server
- IPS wifi-default



Die Änderung der Policy mit **OK** bestätigen.

Hinweis:

Für den Fall dass es sich um verschlüsselten Traffic handelt (bspw. HTTPS), ist es notwendig dass die Fortigate diesen Traffic „aufbricht“ (Deep Inspection) um den eigentlichen Datenverkehr analysieren zu können.

Die hier aufgeführte Lösung dient zur Mitigation der genannten Schwachstelle, bis entsprechende Patches/Konfiguration der betroffenen Endsysteme erfolgt.