

Apache log4j Vulnerability

《持續更新中...》

Dec-14-2021
達友科技

Forcepoint各產品線的影響

- 原廠說明(持續更新)
 - [Apache log4j Zero Day Remote Code Execution Vulnerability CVE-2021-44228 \(forcepoint.com\)](#)

不被此弱點影響

- Forcepoint NGFW
- Forcepoint NGFW VPN Client
- Forcepoint Sidewinder
- Forcepoint Sidewinder Control Center
- **Forcepoint Content Gateway**
- **Forcepoint One Endpoint**
 - Forcepoint DLP Endpoint
 - Forcepoint Web Proxy Connect Endpoint
 - Forcepoint Web Direct Connect Endpoint
 - Forcepoint NGFW ECA Agent
 - Forcepoint CASB Agent
- Forcepoint Bitglass SSE
- Forcepoint Cloud Security Gateway (CSG)
 - Forcepoint Web Cloud Security Gateway
 - Forcepoint Email Security Cloud
- Forcepoint User ID
- Forcepoint Remote Browser Isolation
- Forcepoint Private Access
- Forcepoint Advanced Malware Detection
- Forcepoint Directory Synchronization Client
- Forcepoint Neo Endpoint
- **Forcepoint Email Security**
- Forcepoint Insider Threat

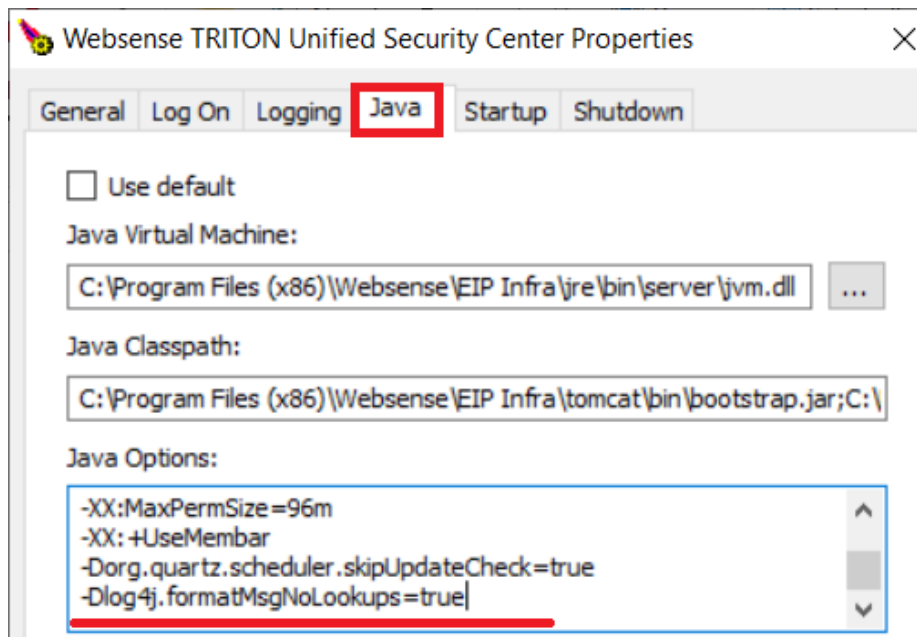
會被此弱點影響

- Forcepoint NGFW Security Management Center Software (see article [38989](#) and associated [Tech Alert](#))
- Forcepoint SMC Appliances (see article [38989](#) and associated [Tech Alert](#))
- **Forcepoint Web Security (Investigation in Progress for Remediation or Mitigation)**
- **Forcepoint DLP (see article [38992](#) and associated [Tech Alert](#))**
- **Forcepoint Security Manager (see article [38991](#) and associated [Tech Alert](#))**
- Forcepoint Behavior Analytics (FBA) (Investigation in Progress for Remediation or Mitigation)
- Forcepoint CASB (Investigation in Progress for Remediation or Mitigation)
- Forcepoint DDP (Investigation in Progress for Remediation or Mitigation)
- Forcepoint Data Protection Service (DPS)
 - **Note** DPS has been updated to mitigate the issue identified in CVE-2021-4228 as of 4:30am Central Time, December 12th. No action is required by Forcepoint customers.
- Forcepoint Dynamic User Protection (DUP)
 - **Note** DUP has been updated to mitigate the issue identified in CVE-2021-4228 as of 9:30am Central Time, December 13th. No action is required by Forcepoint customers.

- Forcepoint Security Manager (EIP) => 1 處
- Forcepoint DLP => 4 處
- Forcepoint OCR => 1 處
- Forcepoint Web Security => 原廠還在清查

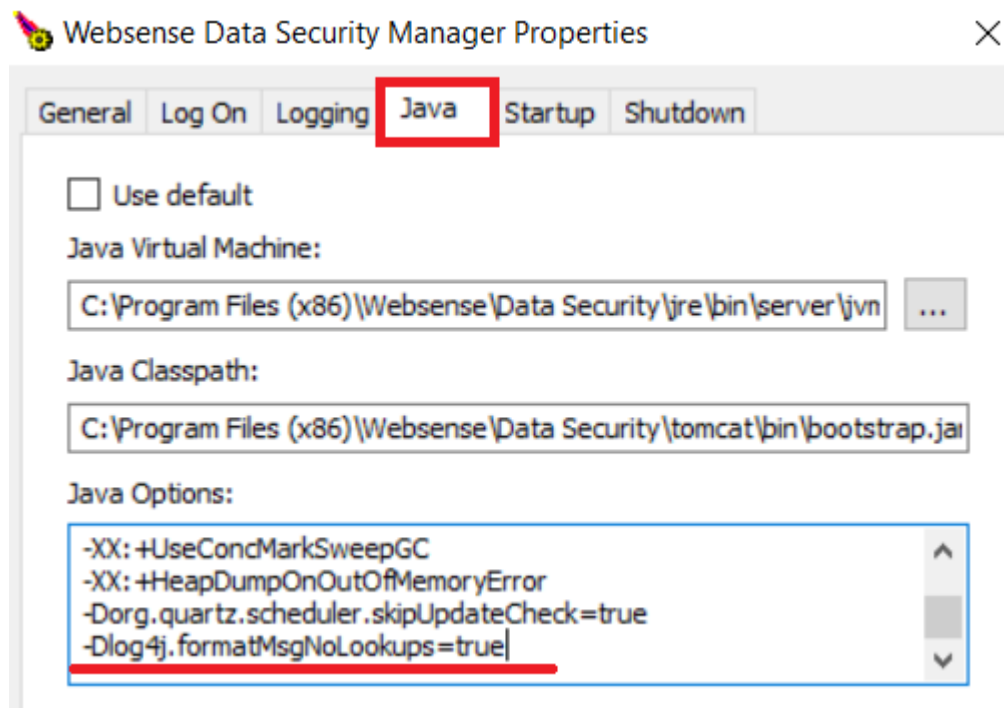
Forcepoint Security Manager (1處)

- 原文(持續更新) : [CVE-2021-44228 Java log4j vulnerability mitigation with Forcepoint Security Manager](#)
- 步驟 :
 - 執行EIPManagerw.exe (X:\Program Files (x86)\ Websense\EIP Infra\tomcat\bin\EIPManagerw.exe)
 - 在Java的頁面中加入 **-Dlog4j.formatMsgNoLookups=true**
*** 上述字串請盡量用複製的方式 · 避免手打錯誤 ***
 - 重啟 Websense TRITON Unified Security Center 服務



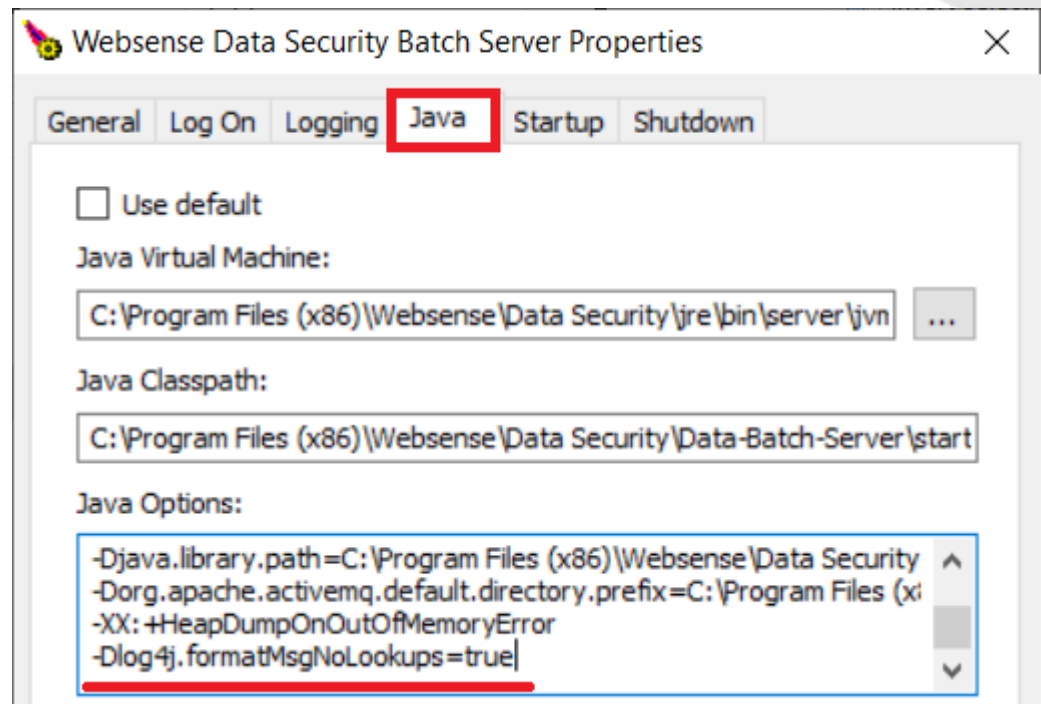
Forcepoint DLP (4處)

- 原文: [CVE-2021-44228 Java log4j vulnerability mitigation with Forcepoint DLP](#)
- Data Security Manager service
 - 執行 %DSS_HOME\tomcat\bin\DSSManagerw.exe
 - 在Java的頁面中加入 -Dlog4j.formatMsgNoLookups=true
 - 重啟 Websense Data Security Manager 服務



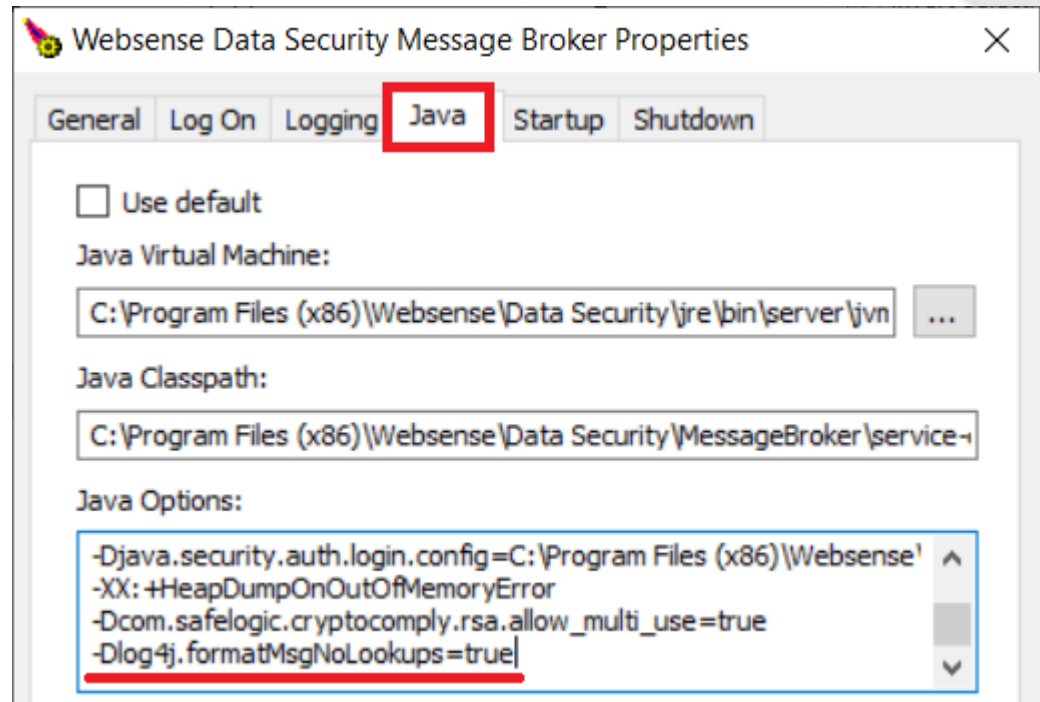
■ Data Security Batch Server service

- 執行%`DSS_HOME`\Data-Batch-Server\service-config\DSSBatchServerw.exe
- 在Java的頁面中加入 `-Dlog4j.formatMsgNoLookups=true`
- 重啟 Websense Data Security Batch Server 服務



■ Data Security Message Broker service

- 執行 %DSS_HOME\MessageBroker\service-config\DSSMessageBrokerw.exe
- 在Java的頁面中加入 **-Dlog4j.formatMsgNoLookups=true**
- 重啟 Websense Data Security Message Broker服務



■ DLP Endpoint Server Connector service

- 到該目錄 %DSS_HOME\EPS_CAMEL\service-config
- 備份原本的 log4j2.xml
- 下載 <https://dl.docutec.biz/forcepoint/log4j2.zip>
- 上述檔案解壓縮後，把log4j2.xml 複製(覆蓋)到該目錄中
- 重啟 Websense DLP Endpoint Server Connector服務

This PC > Local Disk (C:) > Program Files (x86) > Websense > Data Security > EPS_CAMEL > service-config

Name	Date modified	Type	Size
application.properties	22/10/2020 00:21	PROPERTIES File	1 KB
camel.log	11/05/2021 23:50	Text Document	100 KB
eps-camel.jar	24/09/2020 03:35	JAR File	27,413 KB
EPSCconnector.exe	09/09/2020 17:13	Application	102 KB
EPSCconnector32.exe	09/09/2020 17:13	Application	79 KB
EPSCconnectorw.exe	09/09/2020 17:13	Application	102 KB
install-epsconnector-service.bat	09/09/2020 17:13	Windows Batch File	4 KB
log4j2.xml	13/12/2021 22:42	XML Document	2 KB
log4j2.xml.BAK	09/09/2020 17:13	BAK File	2 KB
run-eps-camel.bat	09/09/2020 17:13	Windows Batch File	1 KB
task_list.txt	13/12/2021 22:29	Text Document	0 KB
uninstall-epsconnector-service.bat	24/09/2020 03:22	Windows Batch File	1 KB

Forcepoint OCR (1處)

▪ DLP Endpoint Server Connector service

- 到該目錄 %DSS_HOME\EPS_CAMEL\service-config
- 備份原本的 log4j2.xml
- 下載 <https://dl.docutec.biz/forcepoint/log4j2.zip>
- 上述檔案解壓縮後，把log4j2.xml 複製(覆蓋)到該目錄中
- 重啟 Websense DLP Endpoint Server Connector服務

This PC > Local Disk (C:) > Program Files (x86) > Websense > Data Security > EPS_CAMEL > service-config

Name	Date modified	Type	Size
application.properties	22/10/2020 00:21	PROPERTIES File	1 KB
camel.log	11/05/2021 23:50	Text Document	100 KB
eps-camel.jar	24/09/2020 03:35	JAR File	27,413 KB
EPSCconnector.exe	09/09/2020 17:13	Application	102 KB
EPSCconnector32.exe	09/09/2020 17:13	Application	79 KB
EPSCconnectorw.exe	09/09/2020 17:13	Application	102 KB
install-epsconnector-service.bat	09/09/2020 17:13	Windows Batch File	4 KB
log4j2.xml	13/12/2021 22:42	XML Document	2 KB
log4j2.xml.BAK	09/09/2020 17:13	BAK File	2 KB
run-eps-camel.bat	09/09/2020 17:13	Windows Batch File	1 KB
task_list.txt	13/12/2021 22:29	Text Document	0 KB
uninstall-epsconnector-service.bat	24/09/2020 03:22	Windows Batch File	1 KB

dōcutek