# Log4shell Attack Surface Assessment Tool (Log4j 취약점 평가툴)

**트렌드마이크로에서는 엔드포인트의 Log4j 취약점 존재여부를 확인할 수 있는 툴을 누구나 확인할 수 있도록 하는 서비스를 제공하고 있습니다.**

**이 툴은 Software as a Service(SaaS)의 형태로 제공되며, CVE-2021-44228, CVE-2021-45046, CVE-2021-45105 취약점의 존재여부를 탐지합니다.**

**아래의 URL 에 접속하여 Log4j 취약점 평가 서비스를 이용할 수 있습니다.**

https://resources.trendmicro.com/Log4Shell-Vulnerability-Assessment.html

사용 방법은 아래와 같습니다.

(인터넷 액세스가 가능한 엔드포인트에서만 사용할 수 있습니다.)

1. 위의 URL 에 접속하여 사용자 가입절차를 진행합니다.
   - First Name, Last Name, 이메일주소, 전화번호, 회사명, 직원 수, 국가선택 등을 진행합니다. 이메일주소는 정확히 기재해야 합니다.
   - Data center location 에서는 Singapore 또는 United States 를 선택합니다.

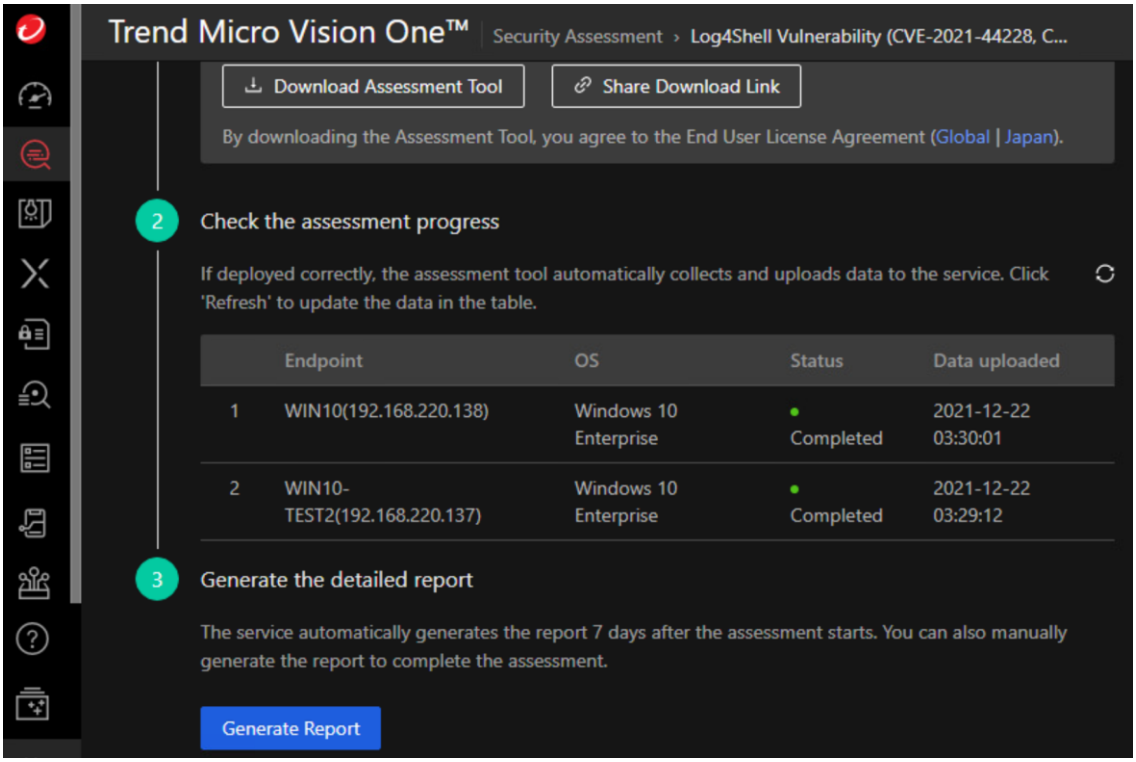
2. 가입 절차를 진행한 후에 [Start]버튼을 클릭하면 트렌드마이크로 Vision One 웹 콘솔에 접속됩니다.

3. Verify Email Address 절차가 진행되는데, 가입절차 당시에 입력했던 이메일 주소의 사서함에 수신된 이메일에서 Verification Code 값을 확인하여 입력합니다. 여섯 자리의 숫자 형태입니다.

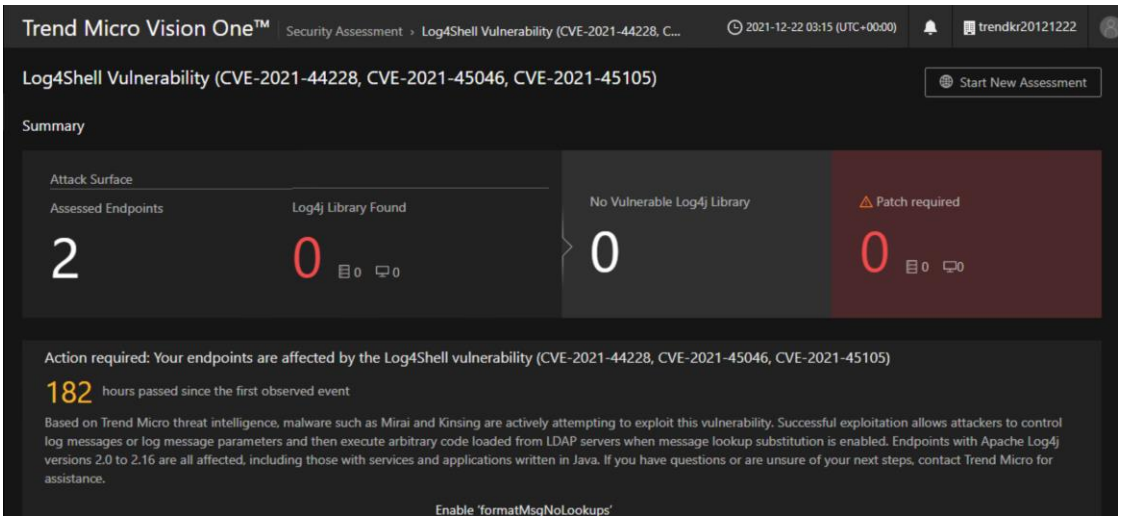
4. 인증 확인 후에 나타나는 Log4Shell Attack Surface Assessment 화면에서 각 플랫폼에 맞는 Assessment Tool 을 다운로드하여 실행하면 해당 엔드포인트에서 취약점 여부를 검색하게 됩니다. 소요시간은 약 1 분 내외입니다. 지원 운영체제는 아래와 같습니다.

- Windows 7, Windows 10, Windows Server 2016 & 2019
- Red Hat Enterprise Linux 6, 7, 8, Amazon Linux, CentOS 6, 7, 8, Ubuntu 16, 18, 20
- MacOS 10.11 이상

5. 다운로드 받은 툴을 다른 엔드포인트에서도 실행하여 취약점 검사를 진행할 수 있습니다.



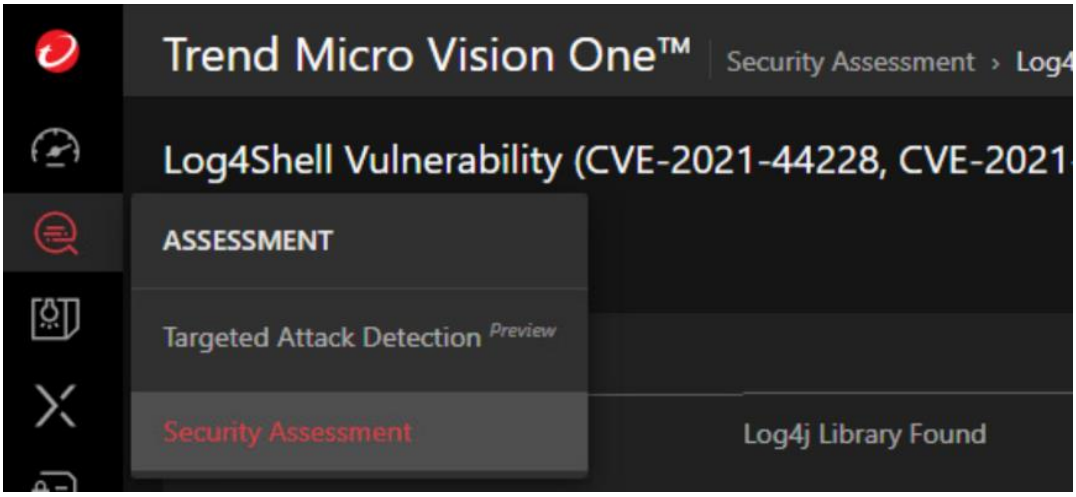

6. 대상 엔드포인트들에서 툴을 실행한 후 수 분이 경과한 후에 웹 콘솔에서 감사 결과를 확인할 수 있습니다.



7. 하단의 [Generate Report]를 클릭하면 Assessment 결과를 요약 형태로 나타납니다. 감사를 수행한 컴퓨터 수, 취약점이 발견된 컴퓨터 수, 패치가 필요한 라이브러리 등의 정보를 확인할 수 있습니다.

8. 우측 상단의 [Start New Assessment]버튼을 클릭하면 다시 Assessment 를 진행할 수 있습니다. 다시 툴을 다운로드 받고 감사 대상 엔드포인트에서 실행하면 됩니다.

9. 모든 작업을 마치고, 웹 콘솔을 LogOut 한 후에 나중에 다시 서비스를 이용하려면 다음의 절차를 진행하면 됩니다.
   - 서비스 가입 직후 배달된 "Your Log4Shell Vulnerability Assessment credentials" 제목의 메일메시지에서 [Access the service]를 클릭합니다.
   - 웹브라우저가 열리고, Reset Password 화면이 나타납니다.
   - 메일사서함을 확인하여 새로 배달된 Verify Email Address 메일에서 Verification Code 값을 입력한 후에 암호를 지정하고 Submit 합니다.
   - 이후 부터는 https://portal.xdr.trendmicro.com 에 접속하여 가입한 이메일주소와 지정한 암호를 이용하여 트렌드마이크로의 Vision One 웹 콘솔에 로그인할 수 있습니다.




   - 로그인 후에 우측 메뉴의 Assessment -> Security Assessment 를 클릭하여 Log4j 취약점 감사를 진행할 수 있습니다.

본 평가툴 사용에 앞서 아래의 사항을 참고하시기 바랍니다.

- 기존의 트렌드마이크로 Vision One 구매고객은 위의 절차를 진행할 필요가 없으며, Vision One 콘솔에 로그인하여 Assessment 메뉴의 보안 감사(Security Assessment)기능을 통하여 Log4j 취약점을 탐지할 수 있습니다.
- 평가툴을 사용하면 EndpointBaseCamp.exe 프로세스가 실행 중 상태가 되며, 윈도우 작업스케쥴러에 등록되어 1 시간 간격으로 반복 실행됩니다.

- EndpointBaseCamp 툴은 일부 최소한의 필수적인 시스템 정보를 트렌드마이크로 클라우드로 전송합니다. 상세한 내역은 아래의 트렌드마이크로 Success Portal 을 참고하시기 바랍니다.
  https://success.trendmicro.com/solution/000286333

- 각 운영체제에서의 EndpointBaseCamp 툴의 삭제는 아래의 내용을 참고하시기 바랍니다.

Windows 용 EndpointBaseCamp 툴 삭제:

https://release-us1.mgcp.trendmicro.com/pkg/app-log4shell-assessment-uninstaller/us1/Log4Shell-Assessment-Uninstall.zip 다운로드 및 압축해제 후 실행

Linux 용 EndpointBaseCamp 툴 삭제:

https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-online-help/assessment-part/security-assessment/deploying-the-assess.aspx 하단 내용 참고

MacOS 용 EndpointBaseCamp 툴 삭제:

https://docs.trendmicro.com/en-us/enterprise/trend-micro-xdr-online-help/assessment-part/security-assessment/deploying-the-assess_001/removing-the-assessm.aspx 내용의 스크립트 실행

기술문의는 support@trendmicro.co.kr 로 메일 주시기 바랍니다.