2018 年 4 月 27 日

サービス＆セキュリティ株式会社 e-Gate センター

注意喚起：WebLogic Server の脆弱性を突いた攻撃について

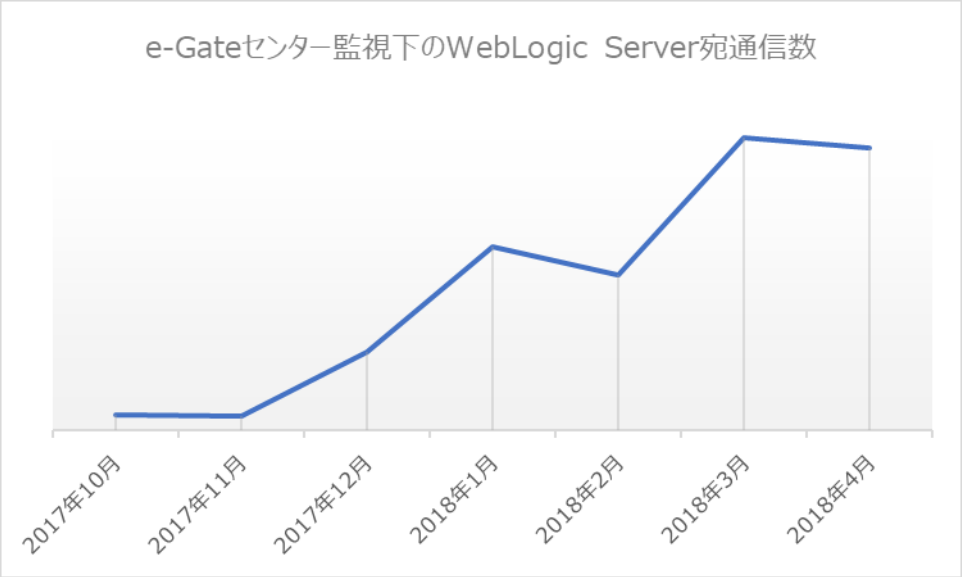
1. 概要

2017 年 12 月下旬より Oracle WebLogic Server[1](以下、WebLogic Server)のサブコンポーネントである WLS Security における脆弱性(CVE-2017-10271)を突く攻撃が報告されております。

この脆弱性は、WLS Security に対して悪意を持った攻撃者が細工したリクエストを送ることで、サーバ実行ユーザ権限で任意のコードを実行可能にすることができるものです。悪用された場合は、情報の搾取や改ざん、DoS 攻撃を受けるといった可能性があります。共通脆弱性評価システム「CVSS v3」におけるスコアは 9.8 と高く、容易に悪用が可能だとされています。昨年末に公表された脆弱性ですが、4 月になった現在でも活発な攻撃活動が観測されております。

当セキュリティオペレーションセンター(以下、e-Gate センター)においても、本脆弱性を狙ったと思われる通信を検知しています。下図は e-Gate センターが監視するシステムにおける当該通信のイベント数のグラフです。2017 年 12 月下旬より多数通信が検知され始め、依然として多くの通信を確認しています。

攻撃の対象とされて被害を受けないようにする為に、対策を実施しなければなりません。正しい情報を把握して早期に対応することが必要です。



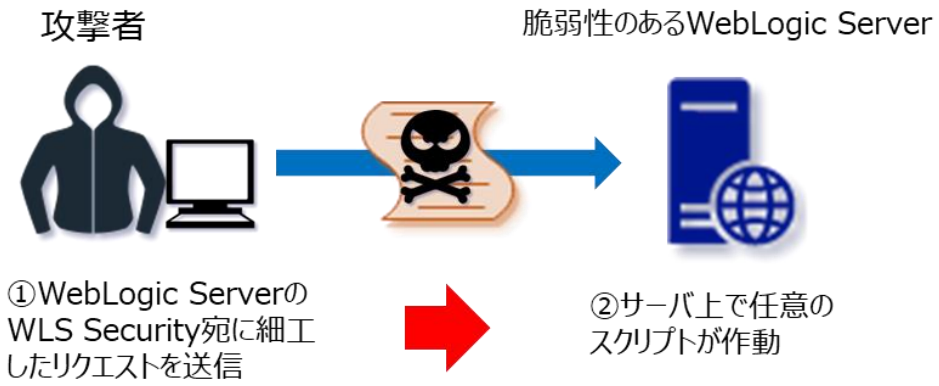
【図 1　WebLogic Server 宛の通信数の推移】

[1] Oracle 社の提供するアプリケーションサーバソフト

2. WebLogic Server の脆弱性を突いた攻撃と対策について

⑴ WebLogic Server の脆弱性を突いた攻撃

攻撃者は脆弱性のある WebLogic Server に対して、細工を施したリクエストを送信し、サーバ上で攻撃者が用意した任意のコードを実行します。



【図 2 攻撃イメージ】

2018 年 4 月現在では、主に仮想通貨をマイニング[2]するプログラムをサーバにダウンロードさせて実行し、サーバのリソースを使用してマイニングを行う攻撃が主流となっています。仮に当該脆弱性を悪用され、マイナー[3]が仕込まれると CPU 使用率が著しく高騰します。CPU の使用率が急騰した場合は、見覚えのない不審なプロセスを停止して下さい。

⑵ 対象

次のバージョンの Oracle WebLogic Server が本脆弱性の影響を受けます。

- Oracle WebLogic Server 10.3.6.0.0
- Oracle WebLogic Server 12.1.3.0.0
- Oracle WebLogic Server 12.2.1.1.0
- Oracle WebLogic Server 12.2.1.2.0

※上記バージョン以外でも脆弱性の影響を受ける可能性があります。詳細はベンダに確認してください。

⑶ 対策

Oracle より、修正済みバージョンが提供されています。

- Oracle WebLogic Server 12.2.1.3.0

修正済みバージョンを適用することを推奨いたします。

---

[2] コンピュータで仮想通貨の取引をチェックし、ブロックチェーンという取引台帳に追記していく作業のこと。

[3] マイニングするプログラム、又はマイニングを行う人を指します。

⑷ 参考情報

JPCERT/CC　Oracle WebLogic Server の脆弱性（CVE-2017-10271）に関する注意喚起
https://www.jpcert.or.jp/at/2018/at180004.html

JVNDB-2017-008734
https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-008734.html

Oracle Critical Patch Update Advisory - October 2017
http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

3. e-Gate の活用について

今回の攻撃は製品の脆弱性を突く攻撃の 1 種です。ターゲットとなるサーバへの攻撃を早期に発見する為には日々の運用監視が重要です。SSK の総合セキュリティサービス「e-Gate」のセキュリティ運用監視サービスをご活用頂くことで精度の高い検知、早期発見による迅速な事後対応が可能となります。

■総合セキュリティサービス　e-Gate
SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。
【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp