【Technical Report18-04】

2018年4月27日
株式会社セキュアソフト

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（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。
弊社グループ会社であるサービス＆セキュリティ株式会社（SSK）のe-Gateセンターから注意喚起のレポートが発行されました。これに関連してセキュアソフト製品の対応状況を公開いたします。

2. SecureSoft 製品の対応について

今回の脆弱性に対応する製品としては、「SecureSoft Sniperシリーズ」が該当いたします。

■SecureSoft Sniperシリーズ
ネットワークを通過するパケットに対して、様々な角度から詳細な分析を行い、攻撃を検知・遮断する事ができる「防御」のための不正侵入検知・防御システム（IPS：Intrusion Prevention System）です。

Sniperシリーズの今回の脆弱性に対応するシグネチャは以下となります。

シグネチャコード	CVEコード	シグネチャ名
3956	CVE-2017-10271	WebLogic CoordinatorPortType RCE
3957	CVE-2017-10271	WebLogic CoordinatorPortType RCE.A
3958	CVE-2017-10271	WebLogic CoordinatorPortType RCE.B
3959	CVE-2017-10271	WebLogic CoordinatorPortType RCE.C
3960	CVE-2017-10271	WebLogic CoordinatorPortType RCE.D
3961	CVE-2017-10271	WebLogic CoordinatorPortType RCE.E
3962	CVE-2017-10271	WebLogic CoordinatorPortType RCE.F
3963	CVE-2017-10271	WebLogic CoordinatorPortType RCE.G
3964	CVE-2017-10271	WebLogic CoordinatorPortType RCE.H
3965	CVE-2017-10271	WebLogic CoordinatorPortType RCE.I

3966	CVE-2017-10271	WebLogic CoordinatorPortType RCE.J
3967	CVE-2017-10271	WebLogic CoordinatorPortType RCE.K
3976	CVE-2017-10271	WebLogic CoordinatorPortType RCE.L
3977	CVE-2017-10271	WebLogic CoordinatorPortType RCE.M
3978	CVE-2017-10271	WebLogic CoordinatorPortType RCE.N
3979	CVE-2017-10271	WebLogic CoordinatorPortType RCE.O
3982	CVE-2017-10271	WebLogic CoordinatorPortType RCE.P
3983	CVE-2017-10271	WebLogic CoordinatorPortType RCE.Q

＊CVE-2018-2628 についても近日中に対応シグネチャをリリース予定です。

今回のような影響範囲の大きい脆弱性問題では対策パッチなどをすべての対象機器に早期に適用する事は容易ではありません。そこで、今回の脆弱性を利用した攻撃から Sniper を利用して防衛ラインを確立しつつ、システムのアップデートを行うことが有効な対応策となります。また、普段から SOC サービスを利用してシステムのセキュリティログ監視により予兆を早期に発見することで被害を最小限にすることも有効な対策となります。ぜひ、セキュアソフトの製品、サービスを活用ください。

■SecureSoft Sniper シリーズ
https://www.securesoft.co.jp/products/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。リンク先のコンテンツは予告なく、変更、削除される場合があります。
※掲載した会社名、システム名、製品名は一般に各社の登録商標 または商標です。

«お問合せ先»
株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp