2021 年 10 月 28 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：情報共有ツール「Confluence」の脆弱性をついた攻撃について

1. 概要

2021 年 8 月に、Atlassian 社から「Confluence Server」および「Confluence Data Center」の脆弱性（CVE-2021-26084）に関するセキュリティアドバイザリが公開されました。

本件の悪用攻撃については、米サイバー軍が 9 月に攻撃規模が急拡大しているとして緊急警告を発しています。国内でも本脆弱性を探索する通信を確認しており、JPCERT/CC が脆弱性に関する注意喚起を発表しています。また、9 月以降 e-Gate センターでも本脆弱性を悪用した攻撃を検知しております。

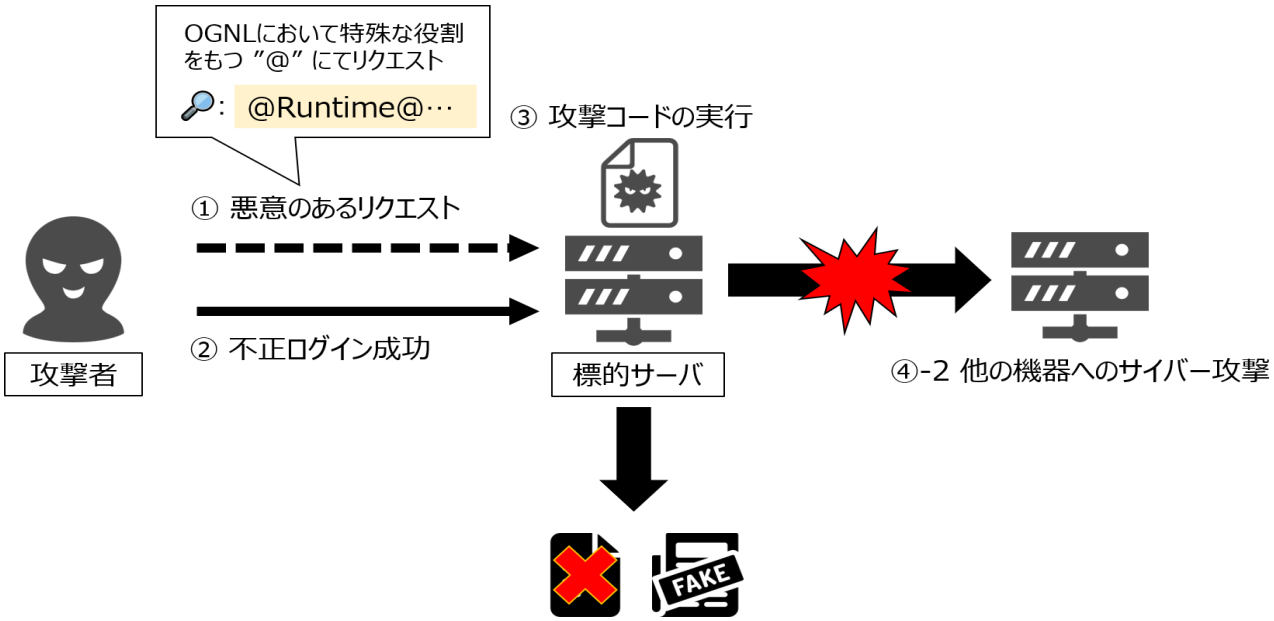
今回はこの脆弱性の詳細、攻撃手法とその対策について紹介いたします。

2. CVE-2021-26084 を悪用した OGNL インジェクション攻撃の詳細

Atlassian 社製品の利用者は世界で 15 万社を超えており、Zoom や Twitter など国内でなじみのある企業も利用しています。その中でも「Confluence」は場所を問わず作業の構築や整理、共有ができるアプリケーションとして、アイティクラウド社主催の「ITreview Grid Award 2020 Spring」においてトップ評価を得ています。また、国内においても多くの企業で導入されており、リモートワークの普及をきっかけに利用者を増やしています。

Atlassian 社は 8 月 25 日に「Confluence Server」および「Confluence Data Center」に OGNL インジェクションの脆弱性が確認されたことを発表し、その脆弱性に関するセキュリティガイダンスを公開しました。その後世界中で脆弱性を悪用した攻撃が確認されています。日本国内においても 9 月にこの脆弱性を探索する通信を確認後、実際に攻撃があったことが確認されています。なお脆弱性対象機器は「Confluence Server」及び「Confluence Data Center」の一部のバージョンであり、「Confluence Cloud」は本脆弱性の影響を受けないとのことです。

この脆弱性を悪用した OGNL インジェクションの攻撃の手法については、図 1 のとおりとなります。



【図 1】OGNL インジェクション攻撃の手法

OGNL(Object Graph Navigation Language)インジェクション攻撃とは、OGNL を利用したシステムへのインジェクション攻撃のことです。OGNL とは Java オブジェクトのプロパティにアクセスしたりメソッドを呼び出したりすることのできる Java によく似た式言語です。OGNL インジェクション攻撃の手法は以下の流れで行われます。

① 攻撃者が本来サーバへ命令を行わない入力ボックスに対して、標的サーバへ OGNL において特定の特殊な役割をもつ文字列を含めた悪意のあるリクエストを入力。

② 攻撃者は情報を窃取し、サーバへの不正ログインを実施。

③ 標的サーバ上で任意のコードを実行。

任意のコード実行には以下のようなものが含まれています。

④-1 重要なファイルの削除・改ざん

サーバの管理者権限を不正取得され、サーバ内のファイルを削除・改ざんされる可能性があります。
これにより提供中のサービスが停止するなどの業務影響が考えられます。

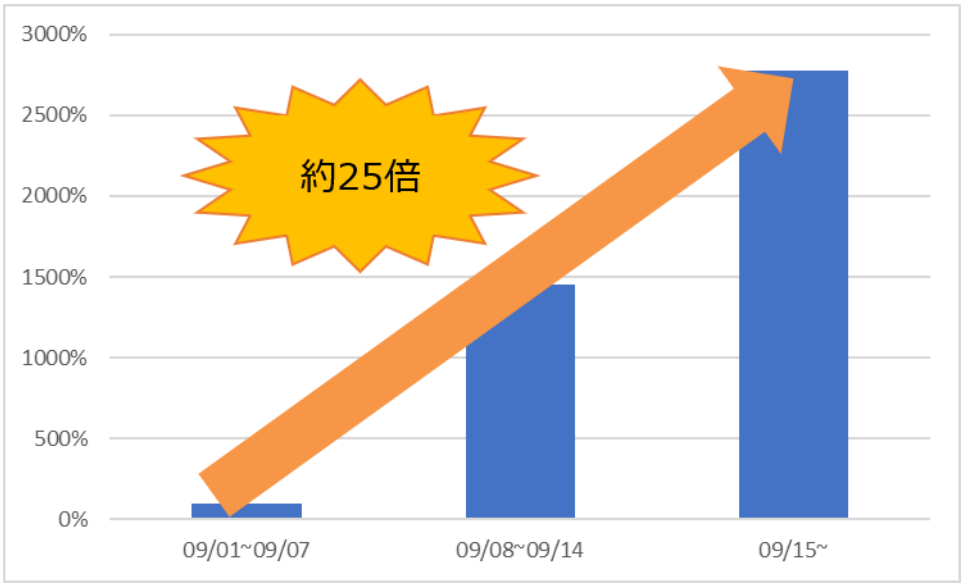
④-2 他の端末への攻撃

標的サーバを踏み台として他端末へのサーバ攻撃を行う可能性があります。

これらは一例ですが、どの攻撃についても攻撃が成功してしまった場合業務への被害は甚大なものとなります。
実際、Atlassian 社はこの脆弱性を CVSS スコアで 10 点満点中 9.8(緊急)と割り当てています。
他にも、暗号資産の採掘を行うマルウェアを設置するなどの攻撃活動に関する情報が公開されています。

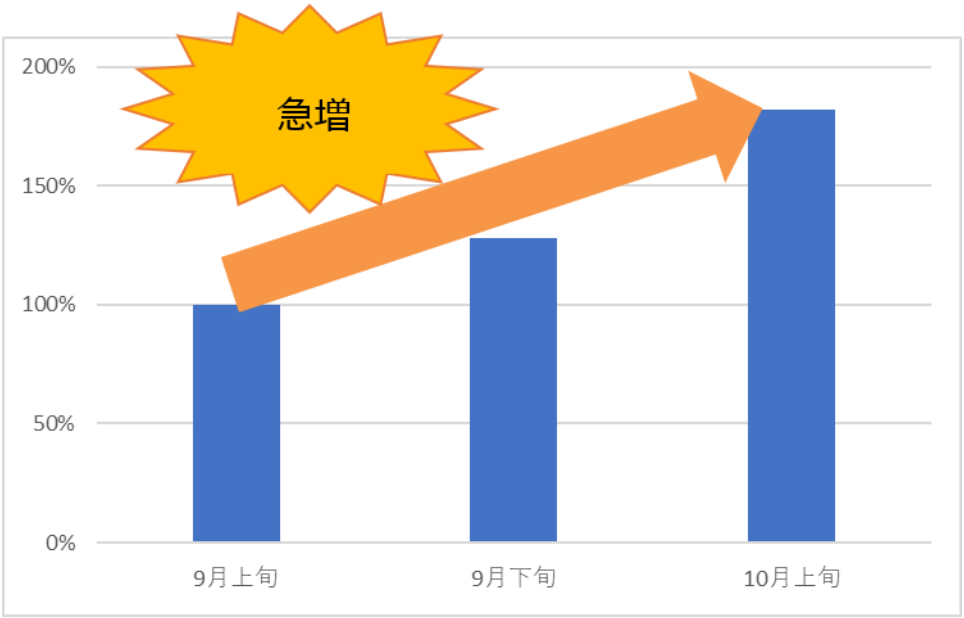
3. e-Gate センターにおける攻撃検知の推移

e-Gate センターでは本脆弱性をついた攻撃を 9 月以降検知しております。
脆弱性が公開されて以降の一か月で爆発的に増加しており、脆弱性に対して素早い対応が求められています。
実際の推移観測結果は図 2 のとおりです。



【図 2】CVE-2021-26084 検知割合

また、インジェクション攻撃に関しましては 9 月以降検知数が増加傾向にあり、引き続き注意が必要です。
実際の推移観測結果は図 3 のとおりです。



【図 3】インジェクション攻撃検知割合

4. 攻撃対策

CVE-2021-26084 およびインジェクション攻撃に関する対策としては以下が挙げられます。

- 最新アップデートの適用

  Atlassian 社から本脆弱性を修正したバージョンが公開されています。十分なテストを実施の上、修正済みバージョンへアップデートすることが推奨されます。

  - Confluence Server および Confluence Data Center 7.13.0
  - Confluence Server および Confluence Data Center 7.12.5
  - Confluence Server および Confluence Data Center 7.11.6
  - Confluence Server および Confluence Data Center 7.4.11
  - Confluence Server および Confluence Data Center 6.13.23

- 緩和策の実行

  Confluence をすぐにアップグレードできない場合は、一時的な回避策として、Linux ベースのシステム向けスクリプトおよび Microsoft Windows ベースのシステム向けスクリプトが提示されており、そちらを実行することで問題を軽減することができます。

- エスケープ処理の実行

  インジェクション攻撃の対策として攻撃を受けやすい検索バーなどの入力マスに対して特殊な役割を持つ特定の文字を普通の文字としてしか機能しないようエスケープ処理をすることも有用です。

- セキュリティ機器による攻撃通信の監視

  WAF(Web Application Firewall)などのセキュリティ機器により、悪意のあるリクエスト送信などの不審な通信を検知・遮断することも一定の効果が見込めます。

- エラーメッセージの非表示化

  悪意のあるリクエストに対してエラーメッセージを表示するとシステムに関するヒントとなってしまう可能性があります。
  そのヒントから実際に攻撃が成功するリクエストを作成される危険があるためエラーメッセージを非表示にすることも対策となります。

本脆弱性を悪用した OGNL インジェクション攻撃に限らずインジェクション攻撃は今後も脅威となり続ける可能性が高いと推測され、攻撃の標的となる可能性があります。

WAF をはじめとしたセキュリティ機器によって攻撃を検知、防御することで被害を最小限にすることやエスケープ処理によって攻撃の被害にあわないようにすることが求められます。特に、攻撃と思われる通信に対していち早く気付き対応できる仕組みを持った監視体制を敷くことはサイバー攻撃の対策として有効です。

5. e-Gate の監視サービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。e-Gate のセキュリティ監視サービスをご活用いただきますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■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」と最新のメソッドで構築した「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”サービスです。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/

6. 参考情報

JPCERT/CC

- Confluence Server および Data Center の脆弱性（CVE-2021-26084）に関する注意喚起
  https://www.jpcert.or.jp/at/2021/at210037.html

ZDNet Japan

- Atlassian「Confluence」の脆弱性攻撃、日本でも発生確認
  https://japan.zdnet.com/article/35176308/

Confluence Support

- Confluence Security Advisory - 2021-08-25
  https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

ITreview Grid Award 2020 Spring

- アトラシアン、製品レビューで法人ユーザーから高評価を獲得
  https://www.atlassian.com/pl/company/news/ja-press-releases/itreview-grid-award-2020-spring

※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»
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