ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●ソースコード管理ツール「GitLab」、世界約5,400台、国内約150台のサーバーに脆弱性

https://news.mynavi.jp/techplus/article/20240127-2870306/
https://securityaffairs.com/158075/hacking/gitlab-servers-vulnerable-cve-2023-7028.html

このニュースをザックリ言うと･･･

- 1月24日(現地時間)、サイバーセキュリティ系メディア「Security Affairs」より、ソースコード管理ツール「GitLab」のサーバーについて、緊急性の高い脆弱性が修正されていないバージョンが全世界で5,379台稼働していると発表されました。

- 脆弱性(CVE-2023-7028)は同11日にバージョン16.7.2等で修正されたもので、悪用により、GitLabユーザーのアカウントを乗っ取られる恐れがあるとされています。

- 発表の時点で日本国内でも149台のGitLabサーバーに脆弱性があるとされており、セキュリティアップデートの適用が呼び掛けられています。

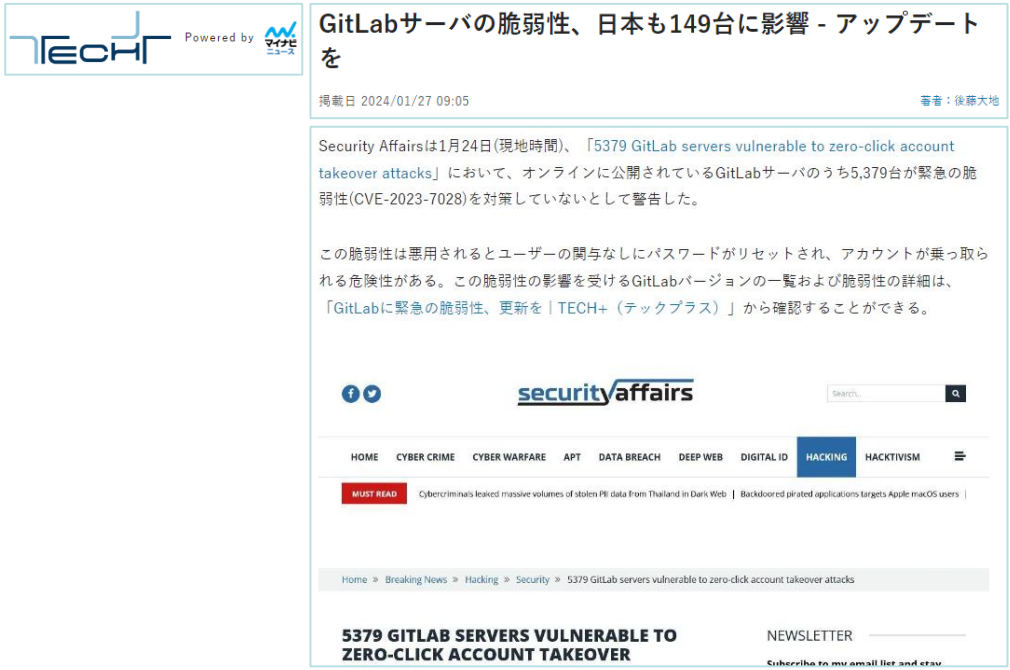
- Security AffairsおよびGitLabの開発元では、アップデート以外の回避策として二要素認証(2FA)を有効にすることも推奨しています。

AUS便りからの所感等

- GitLabはGitHubのようなソースコードのバージョンや開発時の問題追跡等の管理機能を提供するもので、主に各組織でオンプレミスあるいはクラウド上のLinuxサーバーにインストールして使用する形となっています(GitLabではこの他にホスティングサービスも提供しています)。

- バージョン16.7.2(および16.6.4、16.5.6)ではCVE-2023-7028含め5件の脆弱性が修正されていますが、さらに同25日には月例のアップデートとしてバージョン16.8.1(および16.7.4、16.6.6、16.5.8)がリリースされ、ここでも7件の脆弱性が修正されています。

- Linuxディストリビューションでインストールした他のソフトウェアを含め可能な限り最新バージョンに保つようにすることはもちろん、外部からアクセス可能な状態で前述した2FAの利用が難しい場合等には、特定IPアドレスからのみのアクセスに制限することや、前面にUTMやWAFを設置する等も検討に値するでしょう。


TECH+ Powered by マイナビニュース

GitLabサーバの脆弱性、日本も149台に影響 - アップデートを

掲載日 2024/01/27 09:05　著者：後藤大地

Security Affairsは1月24日(現地時間)、「5379 GitLab servers vulnerable to zero-click account takeover attacks」において、オンラインに公開されているGitLabサーバのうち5,379台が緊急の脆弱性(CVE-2023-7028)を対策していないとして警告した。

この脆弱性は悪用されるとユーザーの関与なしにパスワードがリセットされ、アカウントが乗っ取られる危険性がある。この脆弱性の影響を受けるGitLabバージョンの一覧および脆弱性の詳細は、「GitLabに緊急の脆弱性、更新を | TECH+（テックプラス）」から確認することができる。

securityaffairs

HOME CYBER CRIME CYBER WARFARE APT DATA BREACH DEEP WEB DIGITAL ID HACKING HACKTIVISM

MUST READ Cybercriminals leaked massive volumes of stolen PII data from Thailand in Dark Web | Backdoored pirated applications targets Apple macOS users |

Home » Breaking News » Hacking » Security » 5379 GitLab servers vulnerable to zero-click account takeover attacks

5379 GITLAB SERVERS VULNERABLE TO ZERO-CLICK ACCOUNT TAKEOVER

NEWSLETTER

●攻撃者が大企業より小規模な非営利団体を狙う5つの理由

https://dime.jp/genre/1720212/
https://www.crowdstrike.com/blog/reasons-why-nonprofits-are-targets-of-cyberattacks/

このニュースをザックリ言うと･･･

- 1月17日(現地時間)、セキュリティベンダーの米クラウドストライク社より、攻撃者は大企業よりも小規模な非営利団体をターゲットにする、またこれにより非営利団体にとって致命的な被害に繋がるケースがあるとするレポートが発表されました。

- レポートでは、小規模な非営利団体がターゲットになる理由として「サイバー攻撃への防衛が(財政的な制約により)手薄なことを攻撃者は知っている」「低予算のため旧式のPC・OSを利用しているケースが多く(企業・個人から寄付されたPCを利用するケースも)、セキュリティ研修も不足している」「Webサイトで商品・サービスを販売し、購入情報をネットワーク上で管理しており、攻撃者にとってより価値の高いデータを獲得できる可能性がある」「団体が掲げる信条から、政治団体やテロリストの標的になる可能性がある」「より大きなターゲットへアクセスするための踏み台として利用される」の5つを挙げています。

AUS便りからの所感

- レポートはアメリカないし国際的な事情を基にしたものと見受けられますが、日本においても大きな組織がターゲットとされたり、大規模な情報流出等があったりしたものが多く報じられる陰に、中小企業の被害が多くあること、組織が認識しないまま攻撃が成功しているケースもあることは容易に想像できます。

- 例えば5つ目の「より大きなターゲットへアクセスするための踏み台」は、サプライチェーン攻撃や、過去にやり取りしたメールを窃取してビジネスメール詐欺(BEC)を仕掛けること等が考えられ、取引相手に渡すファイルにマルウェアが入り込んだりしないために、各PCでのアンチウイルスによる防御およびUTM等による出口対策、また自分たちが偽メールに騙されないだけでなく相手も被害を受けることがないよう、SPF・DKIM・DMARCといったなりすまし対策を実施する等が大事となります。

@DIME（みんなのライフハック）

サイバー犯罪者が非営利団体を狙う5つの理由

2024.01.17　テクノロジー　#セキュリティ

CrowdStrike（NASDAQ： CRWD）の日本法人であるクラウドストライク合同会社から、非営利団体がハッカーなどのサイバー犯罪者に狙われる5つの理由について解説したリポートが到着したので、その概要をお伝えする。

中小企業（SMB）は大手企業と比較して頻繁にサイバー犯罪の標的になりがちだが、実は小規模な非営利団体は、それよりさらに致命的な被害につながる攻撃の標的になる確率が高いことがわかっているという。

この場合、小さな組織を狙った攻撃が多いというこの傾向は意外に見えるかもしれない。サイバー犯罪者にとって、小規模な非営利団体よりもっと利益を上げられそうな標的があることは明らかだからだ。さらに大規模な民間企業を狙えば、市民から怒りを買う可能性も低くなる。

こうしたリスクがあり、得られる報酬も低いにもかかわらず、非営利団体が専ら標的となる理由は何か。

本リポートでは、非営利団体が標的にされやすい理由を5つ紹介するとともに、致命的な被害につながりかねない攻撃から組織を守る方法についても触れられている。

● 2023年はフィッシングによる不正送金被害急増か…金融庁・警察庁発表

https://scan.netsecurity.ne.jp/article/2023/12/29/50419.html
https://www.fsa.go.jp/ordinary/internet-bank_2.html
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf
https://www.cao.go.jp/others/csi/security/20240130notice.html

このニュースをザックリ言うと･･･

- 12月25日(日本時間)、金融庁と警察庁より、フィッシングによるものとみられるインターネットバンキングによる預金の不正送金被害が急増しているとして注意喚起が出されています。

- 発表によれば、2022年8月下旬から9月にかけて被害が急増して以降は落ち着きを見せていたものの、2023年は2月以降再度被害が増加し、同11月末までにおける被害件数は5,174件、被害額は約80.1億円に上っているとしています。

- 金融庁からは、日々の心がけとして「心当たりのないSMS等は開かない」「身に覚えのない取引を確認した場合は速やかに金融機関に照会する」および「SMS等に記載されたURLからアクセスせず、事前に正しいウェブサイトのURLをブックマーク登録しておき、ブックマークからアクセスする」よう呼び掛けています。

AUS便りからの所感

- 二官庁の他に全銀協と日本サイバー犯罪対策センター(JC3)の四者から、年末年始は特に3大メガバンク(三菱UFJ・三井住友・みずほ)を騙るフィッシングに注意すること、また「不正アクセス」「個人情報の確認」「取引の停止」等のワードに警戒するよう呼び掛けられていました。

- 今年に入っても内閣府を騙り「電力・ガス・食料品価格高騰対応緊急支援給付金(5万円)に関するお知らせ」と題したフィッシングメールが確認され、注意喚起が出されています。

- 上記のような政府機関やセキュリティ関連組織あるいはフィッシング対策協議会等の情報あるいはSNS等での報告を収集し、常に慎重に行動することが重要です。

ScanNetSecurity

脆弱性と脅威／脅威動向

2023.12.29 Fri 8:00

フィッシングによるインターネットバンキングへの不正送金被害が急増、「不正アクセス」「個人情報の確認」「取引の停止」等のワードに注意呼びかけ

警察庁と金融庁は12月25日、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について、注意喚起を発表した。日本サイバー犯罪対策センター（JC3）でも12月25日に、同様の注意を呼びかけている。

シェア　ポスト　送る

警察庁と金融庁は12月25日、フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について、注意喚起を発表した。一般財団法人日本サイバー犯罪対策センター（JC3）でも12月25日に、同様の注意を呼びかけている。

警察庁及び金融庁によると、2023年4月及び8月に、インターネットバンキングに係る不正送金事犯による被害急増に関する注意喚起を行うとともに、被害金融機関と連携し対策を講じているが、その後も被害は拡大し続け、12月8日時点で、2023年11月末における被害件数は5,147件、被害額は約80.1億円と、いずれも過去最多を更新しているという。