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。

●LinuxのPolkitに脆弱性「PwnKit」、ローカルから管理者権限奪取の恐れ

https://japan.zdnet.com/article/35182677/
https://gigazine.net/news/20220127-linux-polkit-bug-gives-attackers-root/
https://blog.qualys.com/vulnerabilities-threat-research/2022/01/25/pwnkit-

このニュースをザックリ言うと･･･

- 1月25日(現地時間)、セキュリティベンダーのQualys社より、多くのLinuxシステムにおいてローカルから管理者権限を奪取可能な脆弱性が存在すると発表されました。

- 脆弱性は「Polkit」と呼ばれるライブラリに存在し、これに含まれるpkexecコマンドを不正に実行することにより、root(Linux/UNIXシステムの管理者権限ユーザー)として任意のコードの実行が可能になるとされています。

- CentOS・Debian・Ubuntu等各Linuxディストリビューションにおいて既にPolkitパッケージの脆弱性を修正したバージョンがリリースされており、アップデートの実施が強く推奨されています(この他、万一アップデートできない場合の緩和策も挙げられています)。

AUS便りからの所感等

- Polkitは管理者権限を持つプロセスが権限を持たないプロセスと通信を行うためのライブラリで、発表によれば、今回の脆弱性はpkexecコマンドが登場した2009年5月の時点で存在していたとのことです。

- 脆弱性については通常リモートからの悪用は不可能とみられる一方、攻撃者がホスト上に侵入した場合に悪用が可能となり、またホストにログイン可能なユーザーが悪意を持っている場合にも脆弱性を突くことは容易と考えられます。

- 多くのLinuxディストリビューションでは、全てのソフトウェアパッケージを一括してアップデートする仕組みが提供されていますので、OSを常に最新に保つために随時これを実行するルーチンを確立すること、またパッケージからではなくソースからコンパイルしたソフトウェアについても、同様に新しいバージョンを確実にインストールする管理体制を整えることが肝要です。

- Linuxを使用するNAS等のアプライアンスでも、Polkitを利用している場合にアップデートがリリースされる可能性があり、これらについてもベンダー情報の確認は必須でしょう。

ZDNet Japan

12年前から存在する「Polkit」の脆弱性、主要な「Linux」ディストリビューションに影響

Steven J. Vaughan-Nichols（Special to ZDNet.com）翻訳校正：編集部　2022-01-27 12:26

Linux関連のセキュリティ脆弱性がまたしても発見された。Linuxカーネルのfs/fs_context.cプログラムに潜んでいたヒープオーバーフローのバグという問題が発見、修正された後、一息つく間もなく新たなセキュリティの問題が見つかった。Qualysが、Polkit（旧称「PolicyKit」）のpkexecに存在する危険なメモリー破壊の脆弱性（CVE-2021-4034）「PwnKit」を発見したと報告している。

この脆弱性の悪用は簡単だという。そして、デフォルト設定の状態で利用できるこの脆弱性を悪用することで、一般ユーザーであっても脆弱なコンピューターで完全なルート権限が得られるようになる。Qualysは概略説明の中で、「この脆弱性は、攻撃者の夢をかなえるものだ」と書いている。

なぜそれほど大きな問題と言えるのだろうか。理由を以下に挙げる。

- pkexecは主なLinuxディストリビューションにデフォルトでインストールされている。
- Qualysによると、「Ubuntu」「Debian」「Fedora」「CentOS」の各ディストリビューションに対するテストで問題が認められており、他のディストリビューションにも問題があるのは間違いないという。

● Androidマルウェア「BRATA」の亜種発生、銀行預金を奪取しスマートフォンを初期化

- https://gigazine.net/news/20220131-android-malware-factory-reset-bank-accounts/

このニュースをザックリ言うと・・・

- 1月24日(現地時間)、セキュリティベンダーのCleafy社より、Androidデバイスに感染するマルウェア「BRATA」の亜種に関する注意喚起が出されています。

- BRATAは2019年に確認されたマルウェアで、当初は感染したデバイスから情報を詐取する等の行為を行うとされていました。

- Cleafyの発表によれば、2021年12月に3種類の亜種「BRATAA」「BRATAB」「BRATAC」を確認しており、オンラインバンキングのログイン情報や銀行アプリの操作情報を窃取し、銀行預金を不正に送金した後でデバイスを工場出荷時の状態に初期化するといった行為を行うとしています。

AUS便りからの所感

- 最初のBRATAはGoogle公式のGoogle Playストアまたはサードパーティーのアプリストアで拡散していた一方、今回の亜種は銀行からの警告を騙るSMSによるフィッシング(スミッシング)等で拡散しているとのことです。

- 現時点では、亜種はイギリス・ポーランド・イタリアあるいはラテンアメリカ(南米)諸国の金融機関をターゲットとすることが確認されていますが、今後日本を含めた国々にも対象が広がることは十分に考えられます。

- 特にSMS上のリンクからアプリをインストールするよう誘導されるケースの大抵はマルウェア感染等を意図したもので、インストールの要求に対して安易に許可しないことが肝要であり、またアプリストアからインストールするケースも含め、デバイス上の権限の利用が不自然に要求された場合にもその場で許可せず、アプリストアやソーシャルネット等での評価・評判を参考として判断するべきです。


2022年01月31日 08時00分 セキュリティ

銀行預金を全て奪った後にスマホをリセットしてくるマルウェアが登場

Androidで3年近く猛威を振るってきたリモートアクセス型トロイの木馬「BRATA」がパワーアップしました。新たに登場したBRATAの亜種は、銀行預金を全て奪い去った上にスマートフォンを工場出荷時の状態に戻す機能が確認されています。

How BRATA is monitoring your bank account | Cleafy Labs
https://www.cleafy.com/cleafy-labs/how-brata-is-monitoring-your-bank-account

Android malware can factory-reset phones after draining bank accounts | Ars Technica
https://arstechnica.com/information-technology/2022/01/android-malware-can-factory-reset-phones-after-draining-bank-accounts/

BRATAは2019年1月にセキュリティ大手のKasperskyが最初に報告したAndroid向けマルウェア。当時確認されていた機能は、スクリーンショットの撮影やロック解除、デバイス情報の窃取、アプリケーションの起動/アンインストール、テキストの送信などで、主にブラジルを中心で拡大したことから「Brazilian Remote Administration Tool Android(ブラジルのAndroid向け遠隔操作ウイルス)」の頭文字を取って「BRATA」と命名されました。

●無償版G Suiteが7月1日終了、有償のGoogle Workspaceサブスクリプションへ移行を

https://www.itmedia.co.jp/news/articles/2201/20/news065.html
https://support.google.com/a/answer/2855120?hl=ja

このニュースをザックリ言うと・・・

- 1月19日(現地時間)、IT系メディアより、Googleが主に企業ユーザーに提供していた「無償版G Suite」が7月1日に終了すると報じられました。

- Googleでは2012年12月に無償版(当時「Google Apps」)について新規申込を終了しており、有償版であるGoogle Workspaceサブスクリプション(当時「Google Apps for Business」)へのアップグレードを促す一方で、既存のユーザーに対する無償版の提供を続けていました。

- Google Workspaceへのアップグレードを5月1日までに行わなかった場合、同日をもって適切なエディションへの切り替わりが行われ、7月1日までに支払い情報を登録しない場合はサービスが一時停止状態に、さらに60日経過でGMail・カレンダー等のコアサービスが利用できなくなるとのことです(支払い情報登録時も7月1日までは無料で利用可能とのことです)。

AUS便りからの所感

- 今回のように、企業・組織内で常用的に利用していた無償サービス等の終了に際し、有償版への移行の提案が通らなかった、あるいは移行等の対応そのものををとらなかった等の理由でそのまま使えなくなることにより、サービスへのアクセスができなくなる、保存していたデータが消失する等で業務に支障をきたすというケースが発生することのないよう、特に管理者においては事前に有償版についての調査を行い、サービスからの通知を見落とさず、早い段階で適宜移行を計画することが重要です。

- 一方で、特にGmailやGoogle Drive等、従業員が個々に(主に無償の)個人用サービスを契約して業務に使用するケースも多々見受けられ、それらへの管理が及ばないまま、社内情報等が持ち出されることへの懸念(AUS便り 2022/01/25号も参照)についても考慮するならば、必要に応じ有償版を正式に契約・提供することも検討すべきでしょう。

ITmedia NEWS

無償版「G Suite」、7月1日に完全終了　有償「Google Workspace」への切り替え推奨

2022年01月20日 07時05分 公開　[佐藤由紀子，ITmedia]

米Googleは、2012年に提供を終了したが既存ユーザーにはそのまま提供してきた従来の無償版「G Suite」を、7月1日に完全に停止する。米9TO5Googleが1月19日（現地時間）、Googleが同日管理者宛に送ったメールに基づいて報じた。

既に管理者向けのヘルプページが更新されている。

まだ従来の無償版G Suiteを使っているユーザーがサービスを継続したい場合、7月1日までに有料の「Google Workspace」にアップグレードする必要がある。最も安価な「Business Starter」プランは1ユーザー当たり月額680円だ。