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。

●OpenSSHに重大な脆弱性、世界約1,400万台のサーバーがリモートから乗っ取りの恐れ

https://www.itmedia.co.jp/news/articles/2407/02/news184.html
https://www.openssh.com/txt/release-9.8
https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server

このニュースをザックリ言うと･･･

- 7月1日(現地時間)、セキュリティベンダーの米Qualys社より、OpenSSHに重大な脆弱性が存在することが発表されました。
- 脆弱性「CVE-2024-6387」はバージョン8.5p1から9.7p1に存在し、悪用により、ログイン権限のない攻撃者にサーバーを乗っ取られる恐れがあるとしています。
- 同社の調査では、世界で約1,400万台のサーバーが脆弱性の影響を受けるとしています。
- 同日、OpenSSHの開発元からは修正バージョン9.8/9.8p1がリリースされており、主要なLinuxディストリビューションにおいてもセキュリティアップデートのリリースが進んでいる他、万が一アップデートできない場合の回避策も提示されています。

AUS便りからの所感等

- 脆弱性は2006年に発見・対策されていましたが、2020年にバージョン8.5p1でこの脆弱性が復活(レグレッション)したことから、「regreSSHion」と命名されています。
- RHELでは、バージョン9のrpmパッケージのみ影響を受ける(8以前では影響を受けない)とのことで、またRocky Linux・Almalinux・Oracle Linux等の派生ディストリビューションにおいては、それぞれ大元のRHELに先立って独自のセキュリティアップデートがリリースされています(現時点ではRHEL 9でも対策済みです)。
- SSHは主にLinuxサーバーをリモートから管理する目的で利用されることから、世界中の攻撃者が日々サービスポート(TCPポート22番)の探索・攻撃を行っており、OpenSSHのアップデートはもちろん、SSHサービスポートへのアクセスを特定のIPアドレスからのみに制限する等の対策をとることも強く推奨されます。

ITmedia NEWS

認証なしでリモートコード実行　OpenSSHに“回帰”した脆弱性「regreSSHion」発覚

2024年07月02日 19時50分 公開　[山川晶之，ITmedia]

セキュリティベンダーの米Qualysは7月1日（現地時間）、SSHソフトウェア「OpenSSH」に重大な脆弱性を発見したと発表した。脆弱性は「regreSSHion」（CVE-2024-6387）と名付けられ、ルート権限で認証なしに任意のコードをリモートで実行できてしまうという。同社によると世界中の1400万台以上のサーバーに影響があるとする。

regreSSHionはOpenSSHサーバで出現するもので、シグナルハンドラーの競合状態で発生。デフォルト構成のsshdが影響を受けるという。脆弱性が悪用された場合、攻撃者はシステムを制御下に置くことができ、マルウェアのインストール、データの改ざん、バックドア作成だけでなく、ネットワーク内にある他システムへの攻撃の足がかりに悪用される恐れがあるとする。

● JavaScriptライブラリ、開発・配布元買収でスクリプト改ざん・マルウェア化の疑い

https://news.mynavi.jp/techplus/article/20240628-2974852/
https://sansec.io/research/polyfill-supply-chain-attack
https://gigazine.net/news/20240702-namecheap-polyfill-io-supply-chain-attack/

このニュースをザックリ言うと・・・

- 6月25日(現地時間)、セキュリティサービス企業のSansec社より、JavaScriptライブラリ「Polyfill .io」の配布元から改ざんされたスクリプトが配布されたとして注意喚起が出されています。
- Polyfill .ioは本来新しいブラウザーのみが対応する機能を古いブラウザーでも使用できるようにするライブラリーでしたが、今年2月に配布サイトや開発者のGithubアカウント等が、CDN等を運営する中国の企業に買収されたことから、スクリプトの改変等が行われる恐れが懸念されていました。
- 改ざんされたスクリプトには、悪意のあるWebサイトに誘導されるようなコードが仕込まれ、実質マルウェア化していたとのことです。
- 後日、Polyfill .ioのサイトはドメイン名を登録していた業者によって停止された模様です。

AUS便りからの所感

- Polyfill .ioの元開発者は、もはや当該ライブラリは必要ないとして、使用を中止するよう呼び掛けていますが、依然需要がある模様で、Cloudflare・Fastly等著名なCDN業者が安全なバージョンの提供を発表しています。
- 外部サイトから自動的に最新のバージョンのスクリプト等を読み込む形にすることで、悪意によるスクリプトの改ざん・アップデート等により、不正なコードが読み込まれてしまう恐れがあることを懸念するのであれば、特定バージョンを指定しての読み込みや、改ざんを検出するSubresource Integrity機構の活用、もしくは予めダウンロードしたスクリプトの設置を検討すべきでしょう。
- サイトを買収した企業は、「polyfillcache .com」という類似したドメイン名で、別のJavaScriptライブラリーを配布するCDNサイトを立ち上げていますが、外見や説明文が既存のCDNサイトに酷似している不審なサイトとなっており、今後またマルウェアを含むスクリプトが配布される恐れがあるため、くれぐれも使用しないように注意しましょう。

TECHR Powered by マイナビニュース

JSライブラリ「Polyfill.io」がマルウェアに改変、10万サイト以上に影響

掲載日 2024/06/28 11:47　　著者：後藤大地

Sansecは6月25日(現地時間)、「Polyfill supply chain attack hits 100K+ sites」において、オープンソースのJavaScriptライブラリ「Polyfill.io」が改変され、10万以上のWebサイトに展開されたと報じた。

Polyfill.ioはAndrew Betts氏が開発した人気のJavaScriptライブラリ。古いWebブラウザをサポートし、JSTOR、Intuit、世界経済フォーラムを含む10万以上のWebサイトに利用されている。

Polyfill.ioは2024年2月、中国を拠点とするコンテンツデリバリーネットワーク(CDN: Content Delivery Network)企業の「Funnull」に買収された。ドメインに加えGitHubアカウントも買収されており、コード改変の可能性があるとして懸念が高まっていた。

●業務委託先でランサムウェア感染、個人情報等61,424件流出

https://www.itmedia.co.jp/business/articles/2407/02/news150.html
https://www.kubota.co.jp/news/2024/data/info20240701.pdf
https://www.iseto.co.jp/news/news_202407.html
https://www.mbs.jp/news/kansainews/20240701/GE00058544.shtml

このニュースをザックリ言うと・・・

- 7月1日(日本時間)、クボタ社および信販子会社のクボタクレジット社より、同社顧客の個人情報が流出したと発表されました。
- 被害を受けたとされるのは、2022年9月度の利用明細および請求書印刷用データに記載された、顧客61,424名(個人・法人・団体名義含む)分の氏名・住所・利用請求明細・引落口座情報の一部とのことで、この他の電話番号等の情報は含まれないとのことです。
- クボタクレジット社が利用明細の印刷・発送を委託していたイセトー社で5月26日にランサムウェア感染が発生、6月18日に攻撃者のサイトにおいて情報流出が確認されたとしています。

AUS便りからの所感

- 一部報道によれば、イセトー社が業務受託していたとされる他の企業・自治体の顧客に関する情報も同様に被害を受けている模様です。
- 国内でのランサムウェア攻撃については、医療機関で度々VPN装置の脆弱性を突かれての侵入・電子カルテデータの暗号化が発生した事案や、6月にKADOKAWAグループが攻撃を受け、今も大規模な障害が発生していること等が話題となっています(KADOKAWAグループの事案については後日取り上げます)。
- それぞれの事案について既に発表されている内容や今後の発表において、攻撃の原因等を分析するとともに、現時点で明確に行うべきこととして、あらゆる機器を最新に保つことや、アンチウイルス・UTM等による防御を固めること、ネットワーク構成やデータバックアップ体制が強固であるかの確認等が重要です。

ITmedia NEWS

クボタ、ランサムウェア被害で6万人の個人情報流出　ネットワークへの影響はなし

2024年07月02日 15時20分 公開　　[ITmedia]

クボタと信販子会社のクボタクレジットは7月1日、クボタクレジットの業務委託先企業のランサムウェア感染により、顧客6万1424人分の個人情報が漏えいしていたと発表した。

クボタクレジットが利用明細などの印刷・発送を委託していたイセトー（京都市）が、5月26日にサーバとPCのランサムウェア感染を確認。調査の結果、6月27日にクボタクレジットの顧客情報流出を確認し、7月1日に漏えいした対象の顧客を特定したという。

漏えいが確認されたのは、2022年9月度の利用明細と、請求書印刷用のデータ。氏名、住所、利用・請求明細、引き落とし口座情報の一部が含まれていた。現時点で、個人情報が悪用されたという報告は受けていないという。